ASA-823

Translation of Japanese Office Action issued on June 22, 2004

The present application is to be rejected for the following ground. If there is any opinion against the ground, a written opinion is to be presented within 60 days after the issue date of this notice.

Ground

The invention according to the following claims of the present application can be easily conceived by those skilled in the art in the technological field of the invention before filing the application based on the invention disclosed in the following publication distributed before the filing date of the present application in Japan or abroad. Therefore, the invention is not patentable pursuant to the provision of Article 29, section 2 of the Japanese Patent Law.

Note (refer to the List of Citations, etc. for referenced citations)

1. Citations 1, 2, 3, and 4 for claims 1 and 3

Citations 1 and 2: Known art to be compared with the entry list

Citation 3: Known art for retrieval by grouping using a hash value

Citation 4: Example of storing not only IDs but also grouping information in media

List of Citations, etc.

1. JP-A-10-187826
2. JP-A-63-298681
3. JP-A-09-091303
4. JP-A-06-274720

No ground of rejection has been detected up to the present time on the inventions according to the claims other than those pointed out in this notice of rejection.

A ground of rejection is reported when it is newly detected.

When any amendment is made, care is to be exercised to make it within the scope of the items described in the specifications or drawings of the present application, and the ground of the amendment is to be stated in the written opinion by clearly pointing out the related descriptions in the specifications or drawings in the filed application.

Record of the search result on the documents of the prior art technology

Field searched IPC 7th version
G06K17/00
G07F 7/08

The record of the search result on the documents of the prior art technology does not configure a ground of rejection.

ASA-823

整理番号　Ｋ９８０１０３０１

発送番号　２１５８９２　1/
発送日　平成１６年　６月２２日

拒絶理由通知書

特許出願の番号	平成１０年　特許願　第２８３７３６号.
起案日	平成１６年　６月　９日
特許庁審査官	奥村　元宏　　８０２２　５Ｎ００
特許出願人代理人	秋田　収喜　様
適用条文	第２９条第２項

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から６０日以内に意見書を提出して下さい。

理　由

この出願の下記の請求項に係る発明は、その出願前日本国内又は外国において頒布された下記の刊行物に記載された発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない。

記　　（引用文献等については引用文献等一覧参照）

１．請求項１、３に対して、引用文献１、２、３、４
　引用文献１、２：登録リストと照合する周知例。
　引用文献３：ハッシュ値でグループ分けして検索を行う周知例。
　引用文献４：ＩＤだけでなくグループ情報も媒体に持たせる例。

引　用　文　献　等　一　覧

１．特開平１０－１８７８２６号公報
２．特開昭６３－２９８６８１号公報
３．特開平９－９１３０３号公報
４．特開平６－２７４７２０号公報

この拒絶理由通知書中で指摘した請求項以外の請求項に係る発明については、現時点では、拒絶の理由を発見しない。
拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

なお、補正する場合は、出願当初の明細書又は図面に記載した事項の範囲内においてなされるよう注意するとともに、意見書において出願当初の明細書又は図面の記載箇所を示して補正の根拠を説明されたい。

－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－－

先行技術文献調査結果の記録

・調査した分野　　ＩＰＣ第７版
Ｇ０６Ｋ１７／００
Ｇ０７Ｆ　７／０８

この先行技術文献調査結果の記録は、拒絶理由を構成するものではない。

この拒絶理由通知の内容に関するお問い合わせ、または面接のご希望がございましたら下記までご連絡下さい。ＦＡＸを送付される場合はＴＥＬで御一報下さい。

特許審査第四部情報処理（記憶管理）　審査官　奥村　元宏
ＴＥＬ　０３（３５８１）１１０１　内線　３５８４
ＦＡＸ　０３（３５０１）０７３７

Translation of Reference 1 (JP-A-10-187826)

(54) Title of Invention: FORGED CARD USE PREVENTING METHOD, CARD READER/WRITER, AND FORGED CARD USE PREVENTING SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To make difficult the use of a forged card without performing any realtime communication with center equipment and any high-level enciphering inside the card.

SOLUTION: When an IC card is used, an ID retrieving means 122 of card reader/writer investigates whether the ID of card is registered on a black list stored in a storage device 130 or not and when that ID is registered, it is discriminated as a forged card. Besides, certifying means 123 communicates with the card to certify the card and when the card is not certified, it is discriminated as a forged card. Communicating means 124 performs non-realtime communication with center equipment, transmits card information to the center equipment and receives the ID to be added to the black list from the center equipment.

[Claims]

[Claim 1]

A forged card use preventing method for preventing unauthorized use of a card, comprising:

transmitting card information such as an ID and a use history, etc. obtained from a card by a card reader/writer to center equipment in non-realtime, evaluating a progress of a use history of a card by center equipment, detecting an ID of a card containing logical inconsistency as a black ID, and transmitting the black ID to the card reader/writer, thereby sequentially updating the black list held by the card reader/writer; and

the card reader/writer detecting an unauthorized card after comparing the card ID with an ID on a black list when a card is used, and identifying through communication with the card, whether or not the card is authorized.

[Claim 2]

A card reader/writer having a function of preventing unauthorized use of a card, comprising:

a control signal interface for performing communications with an external device for providing a service for a user of a card;

a card interface for performing communications with a card;

a communicating device for performing communications with center equipment;

a storage device for storing a black list containing an ID of a forged card transmitted from the center equipment;

card information input/output means for reading card information such as an ID, a use history, etc. stored on a card through the card interface, storing the read information in said storage device,

rewriting the card information based on a predetermined procedure, and writing the rewritten card information to the card through said card interface;

ID retrieving means for checking whether or not the ID of the card is written in the black list stored in said storage device, and, if the ID is detected, issuing a control signal indicating a forged card to said control signal interface;

certifying means for certifying a card by performing communications with the card through said card interface, and, if the card is not certified, transmitting a control signal indicating the forged card to said control signal interface; and

communicating means for performing communications with a center through said communicating device in non-realtime, transmitting card information stored in said storage device to a center, and receiving an ID to be added from the center to the black list.

[Claim 3]

A forged card use preventing system for preventing unauthorized use of a card, comprising:

center equipment, and a plurality of card readers/writers connected to an external device for providing a service for a user of a card and the center equipment as communicable with each other, wherein:

said card reader/writer comprises:

a control signal interface for performing communications with said external device;

a card interface for performing communications with a card;

a storage device;

a communicating device for performing communications with said center equipment;

card information input/output means for reading card information such as an ID, a use history, etc. stored on a card through the card interface, storing the read information in said storage device, rewriting card information based on a predetermined procedure, and writing the rewritten card information to the card through said card interface;

ID retrieving means for checking whether or not the ID of the card is written in the black list stored in said storage device, and, if the ID is detected, issuing a control signal indicating a forged card to said control signal interface;

certifying means for certifying a card by performing communications with the card through said card interface, and, if the card is not certified, transmitting a control signal indicating the forged card to said control signal interface; and

communicating means for performing communications with a center through said communicating device in non-realtime, transmitting card information stored in said storage device to a center, and receiving an ID to be added from the center to the black list,

said center equipment comprises:

a communicating device for performing communications with said card reader/writer;

a storage device;

new history sorting means for rearranging a use history of a newly used card stored in said storage device in an ID order;

merging means for merging a new history with an old history by adding a use history of a newly used card sorted by said new history

sorting means to a use history of a card stored in said storage device and used before;

inconsistency detecting means for evaluating a progress of a use history of a card to which a use history is added, checking whether or not logical inconsistency is detected, and, if inconsistency is detected, registering an ID of the card on a master black list stored in said storage device; and

communicating means for performing communications with said card reader/writer through said communicating device in non-realtime, receiving card information from said card reader/writer and storing the information in said storage device, and transmitting an ID newly registered on said master black list to said card reader/writer, and

said card comprises:

an interface for performing communications with said card reader/writer;

a storage device;

a card information transmitting means for transmitting card information such as an ID, a use history, etc. stored in said storage device to said card reader/writer through said interface;

card information receiving means for receiving new card information from said card reader/writer through said interface, and writing the information to said storage device; and

certifying means for certifying a card by performing communications with said card reader/writer through said interface. [Claim 4]

The forged card use preventing system according to claim 3, wherein

said certifying means of said card reader/writer comprises:

enciphering means for enciphering an input card ID based on an input enciphering key K, and outputting enciphered text;

random number generating means for generating a random number r;

means for transmitting the generated random number r to a card, and receiving output x of a corresponding card;

a selector for selecting a bit string in a position specified by the generated random number r from enciphered text output by the enciphering means and outputting the selected bit string; and

a comparator for comparing output of the selector with the output x of a card; and

said certifying means comprises memory in which data is written in advance, uses a random number r transmitted by said card reader/writer as an address of said memory, and transmits data output x of corresponding memory to said card reader/writer.

[Claim 5]

The forged card use preventing system according to claim 4, further comprising a card signature device comprising: a card interface for performing communications with a card; and means for enciphering the card ID read from a card to be signed through said card interface based on the card ID and a separately input enciphering key, wherein enciphered text obtained by encipherment is written to said memory of a card to be signed through said card interface.

[Detailed Explanation of the Invention]

[0001]

[Field of the Invention in Industry]

The present invention relates to a technology of preventing unauthorized use by forging an IC card for use in making a payment and for identification.

[0002]

[Prior Art]

In our daily life, as it is well-known, a magnetic card and an IC card are widely used as a substitute for cash and an identification card. These cards are frequently used by inserting into a public phone, an automatic gate, an automatic telling machine, etc. without help of a sales person of a store, etc. In such use of the cards, a card can be easily forged by electrically replicating the data of a card on another card without replicating a card with precision. Therefore, a number of malicious users who forge cards and intend to illegally make profits come one after another.

[0003]

In this situation, relating to a credit card, the card information such as the ID, the term of a card, the name of the owner of a card, a use history, etc. is registered and inquired about in the center. An ID refers to a unique number assigned in advance to a card. With the above-mentioned configuration, once the ID of a forged card is registered in the center, the forged card cannot be used any more. The method of thus preventing the unauthorized use of a card is disclosed by, for example, JP-A-3-25568.

[0004]

Furthermore, relating to a credit card, data obtained by enciphering card information such as an ID, etc. is recorded on a card using an enciphering key known only to a card company. Thus, nobody but a staff of a card company can illegally issue a card assigned a new ID. Such a preventing method is disclosed by, for example, JP-A-01-262886 and JP-A-62-188070.

[0005]

A card can be forged by replicating the same card as an authorized card, rewriting the card of an authorized card to enhance the value of the original card (falsification in a narrow sense), producing a card with a new ID (forgery in a narrow sense). In the following case, unless otherwise specified, all illegal related action is referred to as forgery.

[0006]

Certification refers to the technology of identifying whether or not a card is an authorized card by performing communications with the card. Encipherment refers to converting data (plain text) to other data (enciphered text) using an enciphering key, and plain text cannot be easily conceived from enciphered text, or the enciphering key cannot be easily conceived using the enciphered text and the plain text. The certification and the encipherment are explained in detail by, for example, Tsujii, Kasahara, et al "Encipherment and Information Security" published by Shokodo in 1990.

[0007]

[Problems to be Solved by the Invention]

There is the problem with the method of detecting the use of a forged card that a card system used in paying a small amount, not to

mention about a credit card, cannot be applied due to the communications cost required by providing a center and inquiring about the use history of a card. Additionally, there is the problem that, as in the card system used in paying a fare which is to be processed in a short time, the communications with a center cannot be performed because it takes not a short time.

[0008]

Although the conventional method of enciphering an ID of a card and recording it can prevent a forger from freely selecting an ID, but cannot prevent a forger from forging a card. Therefore, it cannot avoid unauthorized use.

[0009]

Furthermore, since the method of preventing unauthorized use of a card only by certification requires a complicated process for encipherment and arithmetic operations on multi-digit integers, it is difficult to perform a high-speed process using an 8-bit microcomputer loaded onto an ID card.

[0010]

The present invention has been developed to solve the above-mentioned problems and aims at providing a forged card use preventing technology capable of performing a high-speed process at a low operation cost.

[0011]

[Means for Solving the Problems]

The present invention is a method for preventing use of a forged card, and includes: transmitting card information such as an ID and a use history, etc. obtained from a card (2 shown in Figure 13) by a card reader/writer (1 shown in Figure 13) to center equipment (3

shown in Figure 13) in non-realtime, evaluating a progress of a use history of a card by center equipment, detecting an ID of a card containing logical inconsistency as a black ID, and transmitting the black ID to the card reader/writer, thereby sequentially updating the black list held by the card reader/writer; and the card reader/writer detecting an unauthorized card after comparing the card ID with an ID on a black list when a card is used, and identifying whether or not the card has been authorized through communication with the card whether or not the card is authorized.

[0012]

A card reader/writer according to the present invention having a function of preventing unauthorized use of a card, includes: a control signal interface (110 shown in Figure 1) for performing communications with an external device (4 shown in Figure 13) for providing a service for a user of a card; a card interface (140 shown in Figure 1) for performing communications with a card; a communicating device (150 shown in Figure 1) for performing communications with center equipment; a storage device (130 shown in Figure 1) for storing a black list containing an ID of a forged card transmitted from the center equipment; card information input/output means (121 shown in Figure 1) for reading card information such as an ID, a use history, etc. stored on a card through the card interface, storing the read information in the storage device, rewriting the card information based on a predetermined procedure, and writing the rewritten card information to the card through the card interface; ID retrieving means (122 shown in Figure 1) for checking whether or not the ID of the card is written in the black list stored in the storage device, and, if the ID is detected, issuing a control signal indicating a forged card

to the control signal interface; certifying means (123 shown in Figure 1) for certifying a card by performing communications with the card through the card interface, and, if the card is not certified, transmitting a control signal indicating the forged card to the control signal interface; and communicating means (124 shown in Figure 1) for performing communications with a center through the communicating device in non-realtime, transmitting card information stored in the storage device to a center, and receiving an ID to be added from the center to the black list.

[0013]

The present invention is also a system for preventing use of a forged card, and includes: center equipment (3 shown in Figure 13), and a plurality of card readers/writers (1 shown in Figure 13) connected to an external device (4 shown in Figure 13) for providing a service for a user of a card (2 shown in Figure 13) and the center equipment as communicable with each other. The card reader/writer includes: a control signal interface (110 shown in Figure 1) for performing communications with the external device; a card interface (140 shown in Figure 1) for performing communications with a card; a storage device (130 shown in Figure 1); a communicating device (150 shown in Figure 1) for performing communications with the center equipment; card information input/output means (121 shown in Figure 1) for reading card information such as an ID, a use history, etc. stored on a card through the card interface, storing the read information in the storage device, rewriting card information based on a predetermined procedure, and writing the rewritten card information to the card through the card interface; ID retrieving means (122 shown in Figure 1) for checking whether or not the ID of the card

is written in the black list stored in the storage device, and, if the ID is detected, issuing a control signal indicating a forged card to the control signal interface; certifying means (123 shown in Figure 1) for certifying a card by performing communications with the card through the card interface, and, if the card is not certified, transmitting a control signal indicating the forged card to the control signal interface; and communicating means (124 shown in Figure 1) for performing communications with a center through the communicating device in non-realtime, transmitting card information stored in the storage device to a center, and receiving an ID to be added from the center to the black list. The center equipment includes: a communicating device (650 shown in Figure 6) for performing communications with the card reader/writer; a storage device (630 shown in Figure 6); new history sorting means (621 shown in Figure 6) for rearranging a use history of a newly used card stored in the storage device in an ID order; merging means (622 shown in Figure 6) for merging a new history with an old history by adding a use history of a newly used card sorted by the new history sorting means to a use history of a card stored in the storage device and used before; inconsistency detecting means (623 shown in Figure 6) for evaluating a progress of a use history of a card to which a use history is added, checking whether or not logical inconsistency is detected, and, if inconsistency is detected, registering an ID of the card on a master black list stored in the storage device; and communicating means (624 shown in Figure 6) for performing communications with the card reader/writer through the communicating device in non-realtime, receiving card information from the card reader/writer and storing the information in the storage device, and transmitting an ID newly

registered on the master black list to the card reader/writer. The card includes: an interface (410 shown in Figure 4) for performing communications with the card reader/writer; a storage device (430 shown in Figure 4); a card information transmitting means (421 shown in Figure 4) for transmitting card information such as an ID, a use history, etc. stored in the storage device to the card reader/writer through the interface; card information receiving means (422 shown in Figure 4) for receiving new card information from the card reader/writer through the interface, and writing the information to the storage device; and certifying means (423 shown in Figure 4) for certifying a card by performing communications with the card reader/writer through the interface.

[0014]

The certifying means of the card reader/writer includes: enciphering means (1102 shown in Figure 11) for enciphering an input card ID based on an input enciphering key K, and outputting enciphered text; random number generating means (1101 shown in Figure 11) for generating a random number r; means (1107 and 1108 shown in Figure 11) for transmitting the generated random number r to a card, and receiving output x of a corresponding card; a selector (1103 shown in Figure 11) for selecting a bit string in a position specified by the generated random number r from enciphered text output by the enciphering means and outputting the selected bit string; and a comparator (1104 shown in Figure 11) for comparing output of the selector with the output x of a card. The certifying means includes memory (1002 shown in Figure 10) in which data is written in advance, uses a random number r transmitted by the card reader/writer as an

address of the memory, and transmits data output x of corresponding memory to the card reader/writer.

[0015]

The system further includes a card signature device including: a card interface (1202 shown in Figure 12) for performing communications with a card; and means (1201 shown in Figure 12) for enciphering the card ID read from a card to be signed through the card interface based on the card ID and a separately input enciphering key K, wherein enciphered text obtained by encipherment is written to the memory of a card to be signed through the card interface.

[0016]

[Operation]

The conventional forged card use preventing technology has been designed to aim at detecting without fail the use of a forged card. However, to detect without fail the use of a forged card inevitably increases the cost of preventing the unauthorized use, and prolongs the time required in detecting the unauthorized use. Then, the present invention has changed the idea and aimed at detecting the use of a forged card at a higher probability. In a case where a large amount of money is paid in one transaction using a credit card, etc., there is the possibility that a user of a forged card purchases a number of expensive goods and then flees somewhere. Therefore, the use of a forged card has to be detected without fail. However, in a system where the amount of payment per transaction is small (a prepaid system for a street bus, subway, etc.), it is not necessary to detect each use of a forged card without fail because a user of this type of forged card has to frequently use the forged card to make a large profit from it. Therefore, a forged card has to be detected once in some times

of unauthorized use of a forged card so that the forged card is detected someday. Furthermore, in a system for arresting a user of a forged card (for example, a system of paying a fare using a card), the loss in the past due to the use of the forged card can be covered by collecting the penalty from a user. It is obvious that the unauthorized use of a forged card can be overlooked at a high probability if the use of a forged card cannot be detected without fail. For example, when a malicious authorized user illegally increases the balance of his or her prepaid card, the card can be illegally used one or several times. However, in such cases, the loss due to the use of a forged card is very small, and the profit of the manager of the card system is not badly damaged even though the unauthorized use cannot be detected. Furthermore, although it may not psychologically tolerable to probably overlook the unauthorized use of a forged card, the important object is to minimize the total amount of the "cost of preventing unauthorized use" and the "loss produced by use of a forged card" rather than to minimize only the "loss due to use of a forged card" without considering the "cost of preventing unauthorized use" with the profits of the manager of the card system taken into account. Therefore, if the "cost of preventing unauthorized use" can be largely reduced according to the present invention, the above-mentioned overlook can be economically admitted.

[0017]

Then, according to the present invention, first in the unauthorized use preventing system using a center, the description standard is lowered. That is, according to the card reader/writer of the present invention, the communications are not performed with the center equipment each time a card is input, but it is checked

whether or not the ID of the input card is registered on the black list stored in the storage device of the card reader/writer, and a forged card is determined if the ID is detected on the black list. The card reader/writer transmits card information such as the ID of the card, the use history, etc. to the center equipment. The transmission to the card reader/writer can be performed each time a card is input to the card reader/writer, at predetermined time intervals, when a predetermined amount of card information is accumulated, or when the center equipment communicates with the card reader/writer. When the communications cost is large, the ID and the use history of only a part of cards can be transmitted without transmitting the IDs and the use histories of all cards. Then, the center equipment determines whether or not a forged card has been used according to the card information about the ID and the use history of a card transmitted from the card reader/writer. If a forged card is detected, the ID of the forged card is registered on the master black list of the center equipment. The center equipment periodically communicates with the card reader/writer, transmits a new ID added to the master black list from the previous communication up to the current point, and registers the black list. Thus, since it is not necessary to perform communications between the center equipment and the card reader/writer in realtime, the communications cost can be reduced, and the time required in determining the unauthorized use can be shortened. In the above-mentioned process, it is obvious that the unauthorized use of a forged card can be overlooked until the ID of the forged card is registered on the black list of the card reader/writer. However, if the amount of one transaction of the card is small, and the interval of the update time of a black list is not

longer, the loss due to the unauthorized use of a forged card can be reduced to a tolerable extent.

[0018]

The above-mentioned "unauthorized use preventing method using a center" has no sufficient preventive effect, and if a large number of forged cards are used, severe economical damage occurs and it becomes difficult to correctly manage the card system. In the present invention, since a black list of the card reader/writer are not instantaneously updated, a card forger can taps the communications between an authorized card and the card reader/writer, generates a forged card according to the card information obtained by the tapping, and uses the forged card. In the card system using a non-contact IC card, forgery can be easily performed through tapping. It is certain that the forged card can be used as an authorized card only until the black list is updated. However, therefore, the card forger obtains a large number of IDs to produce a large number of forged cards. When the forged cards are used and the IDs are registered on the black list of the card reader/writer, a number of authorized cards cannot be used. If there are a large number of IDs maliciously used by a card forger, authorized cards are frequently determined as forged cards. Therefore, the function of the card system may become paralyzed. The "unauthorized use preventing method using a center" has not been practically used, which may be due to the above-mentioned reasons.

[0019]

Then, the present invention uses the "unauthorized use preventing method using certification" in addition to the above-mentioned "unauthorized use preventing method using a center" to detect the unauthorized use of a forged card. Using the certification apparently

disables economy and an effect of preventing unauthorized use to work together first because the current certifying technology can make unauthorized use difficult, and an certifying method with an effect of preventing unauthorized use does not require an additional use of a center, and second because a certifying method capable of easily realizing a device for use with the method goes well with economy, but the detecting technology seems to have no effect of preventing unauthorized use. However, according to the present invention, it is only necessary to detect the unauthorized use of a forged card by certification in a short time until the black list of the card reader/writer is updated, and the unauthorized use of a forged card has to be detected at a higher probability because of above reasons. Therefore, a concise certifying method can be used.

[0020]

[Embodiments of the Invention]

Then, the embodiments of the present invention are described below in detail.

[0021]

Figure 13 shows the entire configuration showing an example of a forged card use preventing system according to the present invention. The forged card use preventing system is configured by a plurality of card readers/writers 1 and center equipment 3 capable of communicating with the plurality of card readers/writers 1 by cable or wireless. The reference numeral 2 designates a card, and the reference numeral 4 designates an external device (for example, a vending machine, an automatic gate, etc.) for providing a service for a user of the card 2.

[0022]

In the forged card use preventing system according to the present embodiment, the card information such as an ID, a use history, etc. obtained from the card 2 by each card reader/writer 1 is transmitted to the center equipment 3 in non-realtime, the center equipment 3 evaluates the progress of the use history of the card, detects the ID of a card containing logical inconsistency as a black ID, and transmits it to the card reader/writer 1, thereby sequentially updating the black list held by each card reader/writer 1. The use history in the card information contains the information (for example, the number assigned to each card reader/writer, etc.) for determination of a card use date and place, a used amount of money, etc. When the card 2 is used, each card reader/writer 1 detects an unauthorized card by comparing the ID of the card with the ID on the black list, and certifies for identifying whether or not the card is an authorized card by communication with the card 2. When a forged card is determined, a control signal is output to the external device 4 to prevent unauthorized use by a forged card by performing a process of rejecting the card, and issuing a warning by the external device 4.

[0023]

Described below are examples of the configurations of the card reader/writer 1, the card 2, and the center equipment 3.

[0024]

Figure 1 is a block diagram showing the basic configuration of the embodiment of the card reader/writer. The card reader/writer of the embodiment is configured by the control signal interface (hereinafter referred to as a control signal IF for short) 110, the

data processing device 120, the storage device 130, the card interface (hereinafter referred to as a card IF for short) 140, and the communicating device 150.

[0025]

The control signal IF 110 is a circuit for communication between an external device for providing a service for a user of a card such as a vending machine, an automatic gate, etc. and the data processing device 120. The card IF 140 is a circuit for communications between a card and the data processing device 120. The storage device 130 is configured by random access memory and read only memory (hereinafter referred to as ROM), stores the data output by the data processing device 120, and provides the stored data in the data processing device 120. The communicating device 150 performs communications between the center and the data processing device 120.

[0026]

The data processing device 120 is configured by a microprocessor, and controls the entire card reader/writer at an instruction written in ROM in advance. That is, in the data processing device 120, the card information input/output means 121 for reading information such as an ID and a use history stored in a card through the card IF 140, storing the read information in the storage device 130, rewriting the use history about the card information according to the information such as the fare, the current date and time, etc. provided through the control signal IF 110 from the device for providing a service for a user of a card such as a vending machine, an automatic gate, etc. as necessary, and writing the rewritten data to the card through the card IF 140; an ID retrieving means 122 for checking whether or not the ID of the card is detected in the black list stored in the storage

device 130, and, if it is detected, transmitting to the control signal IF 110 a control signal indicating that the card is a forged card; the certifying means 123 for certifying a card by communicating with a card through the card IF 140, and transmitting a control signal indicating a forged card to the control signal IF 110 if the card is not certified; and the communicating means 124 for communicating with the center through the communicating device 150, transmitting the card information stored in the storage device 130 to the center, receiving an ID to be added to the black list from the center, and adding it to the black list are realized by the instruction written in the ROM in advance.

[0027]

Figure 2 is a flowchart for explanation of the operation of detecting a forged card in the operations of the card reader/writer shown in Figure 1. In Figure 2, when the card IF 140 provides a control signal indicating that a card has been input for the data processing device 120, the data processing device 120 first reads the information such as an ID, a use history, etc. stored in the card through the card IF 140, stores the information in the storage device 130, rewrites the card information as necessary according to the information such as the fare, etc. provided from the operation of providing a service for a user of a card such as the vending machine, automatic gate, etc., and writes the rewritten data to the card through the card IF 140 (201). Then, the ID retrieving means 122 checks whether or not the ID of the card is detected on the black list stored in the storage device 130 (202). If it is detected, control is passed to the procedure 206. Otherwise, control is passed to the procedure 204 (203).

[0028]

In the procedure 204, the data processing device 120 certifies the card through communications with the card through the card IF 140 using the certifying means 123. If the card is not certified, then control is passed to the procedure 206. Otherwise, the process terminates (205). On the other hand, in the procedure 206, the data processing device 120 transmits a control signal indicating a forged card to the control signal IF 110, thereby terminating the process.

[0029]

Figure 3 is a flowchart for explanation of the operation relating to the communications with the center in the operations of the card reader/writer shown in Figure 1. In Figure 3, when the communicating device 150 provides a control signal indicating that communications from the center have been received for the data processing device 120, the data processing device 120 communicates with the center through the communicating device 150 using the communicating means 124, transmits the card information stored in the storage device 130 to the center (301), and erases the card information stored in the storage device 130 (302). Then, it receives the ID to be added to the black list from the center (303), registers the received ID in the black list stored in the storage device 130 (304), thereby terminating the process.

[0030]

Figure 4 is a block diagram showing the basic configuration of the embodiment of a card. The embodiment of the card is configured by an interface (hereinafter referred to as an IF for short) 410, a data processing device 420, and a storage device 430.

[0031]

The IF 410 is a circuit for communications between the card and the card reader/writer. The storage device 430 is configured by random access memory and ROM, stores the data output by the data processing device 420, and provides the stored data in the data processing device 420.

[0032]

The data processing device 420 is configured by a microprocessor, and controls the card at an instruction written in advance in the ROM. That is, the data processing device 420 is realized as a card information transmitting means 421 for transmitting the information such as an ID, a use history, etc. stored in the storage device 430 to the card reader/writer through the IF 410, a card information receiving means 422 for receiving new card information from the card reader/writer through the IF 410 and writing the information to the storage device 430, and a certifying means 423 for certifying a card by performing communications with the card reader/writer through the IF 410 by an instruction written in advance in the ROM. The certification is described later in detail, but the certifying means 423 according to the present embodiment does not require complicated process. Therefore, the data processing device 420 can be realized by an 8-bit low performance microprocessor.

[0033]

Figure 5 is a flowchart for explanation of the operation of a card shown in Figure 4. In Figure 5, when a control signal requiring communications is provided from the card reader/writer through the IF 410 to the data processing device 420, the data processing device 420 allows the card information transmitting means 421 to transmit

the information such as an ID, a use history, etc. stored in the storage device 430 to the card reader/writer through the IF 410 (501), receives new card information from the card reader/writer through the IF 410 using the card information receiving means 422, and writes it to the storage device 430 (502). Then, the certifying means 423 certifies a card by communications with the card reader/writer through the IF 410 (503), thereby terminating the process. The certifying method is described later in detail, but the certification in the procedure 503 corresponding to but not the same as the certification in the procedure 204 shown in Figure 2 in the card reader/writer.

[0034]

Figure 6 is a block diagram of the function showing the basic configuration of the embodiment of the center equipment. The center equipment according to the embodiment is configured by a data processing device 620, a storage device 630, and a communications device 650.

[0035]

The storage device 630 is configured by random access memory, and ROM, stores data output by the data processing device 620, and provides the stored data for the data processing device 620. The communications device 650 performs communications between the data processing device 620 and the card reader/writer.

[0036]

The data processing device 620 is configured by a microprocessor, and controls the center equipment at an instruction written to the ROM in advance. That is, the data processing device 620 comprises a new history sorting means 621 for rearranging the use history of a newly used card stored in the 630, merging means 622 for merging

a new history and an old history for adding a use history of a newly used card to a use history of cards used in the past and stored in the storage device 630, inconsistency detecting means 623 for evaluating the progress of the use history of cards for the cards whose use history is added, checking whether or not logical inconsistency exists, and, if inconsistency is detected, registering the ID of the card in the master black list stored in the storage device 630, and communications means 624 for communicating with the card reader/writer through the communications device 650, receiving card information from the card reader/writer, storing it in the storage device 630, and transmitting a newly registered ID (black ID) on the master black list to the card reader/writer, which are realized at instructions written in advance in the ROM.

[0037]

Figure 7 is a flowchart for explanation of the operation relating to the detection of a forged card in the operations of the center equipment shown in Figure 6. In Figure 7, the data processing device 620 first rearranges the use history of newly used cards stored in the storage device 630 in an ID order using the new history sorting means 621 (701). Then, the merging means 622 for merging a new history and an old history adds a use history of a newly used card to the use history of cards used in the past and stored in the storage device 630 (702). Then, the inconsistency detecting means 623 evaluates the progress of the use history about the card on which the process in the procedure 703 has not been performed, checks whether or not logical inconsistency exists (703), passing control to the procedure 705 if inconsistency is detected, and passing control to the procedure 706 if inconsistency is not detected (704). Logical inconsistency can

be, for example, using cards having the same IDs at substantially the same time in different places (different card reader/writers), etc.

[0038]

Then, in the procedure 705, the ID of a card in which inconsistency is detected is registered in the master black list stored in the storage device 630 (705), and control is passed to the procedure 706. In the procedure 706, it is checked whether or not the procedure 703 has been performed on all cards whose use history has been added. If the procedure 703 has been performed on all cards whose use histories have been added, then control is terminated and otherwise passed to the procedure 703.

[0039]

Figure 8 is a flowchart for explanation of the operation relating to the communications with the card reader/writer in the operations of the center equipment shown in Figure 6. In Figure 8, the data processing device 620 first starts communications with the card reader/writer through the communications device 650 using the communications means 624 (801), then receives the card information about a newly used card from the card reader/writer (802), transmits a black ID newly registered in the master black list to card readers/writers (803), checks whether or not the communications with all card readers/writers have been performed. If the communications with all card readers/writers have been completed, the process is terminated. Otherwise, a new card reader/writer is selected, and control is passed to the procedure 801 (804).

[0040]

Described below is the certification performed between the card reader/writer and a card.

[0041]

Figure 9 is a chart of the sequence of the certifying method used in the certifying means 123 of the card reader/writer shown in Figure 1 and the certifying means 423 of a card shown in Figure 4. In Figure 9, first, the card reader/writer generates a random number r (901), and transmits the random number r to a card i (902). The i refers to the ID of the card. The card i receives a random number r from the card reader/writer (902), obtains output x acquired by inputting the random number r to a function S1 (903), and transmits x to the card reader/writer (904). The card reader/writer receives x (904), inputs the random number r to the function S1, compares the obtained output with x (905). If they match, it is determined that the card of the partner is an authorized card. Otherwise, it is determined that the card of the partner is a forged card. The function S1 is a function unique to the card I, and the card I has the function S1 only. The card reader/writer has the function Si of the card I for all i.

[0042]

Figure 10 is a block diagram showing an example of the configuration of the certifying means 423 shown in Figure 4. In the present invention, it is only necessary to detect a forged card at a predetermined probability, but it is not necessary to find unauthorized use every time it is made. Therefore, the number the input/output bit of the function Si can be reduced. In the embodiment shown in Figure 10, relating to the function Si, an 8-bit random number r transmitted from the card reader/writer is input to the function Si 1002 through the input terminal 1001, and the 8-bit output x output to the output terminal 1003 is transmitted to the card reader/writer.

Since the number of input/output bits of the function Si is only 8 bits, the function Si 1002 can be configured by only a 256-byte (1 byte = 8 bits) ROM (once-writable ROM). That is, the 256-byte function Si is held in the ROM, an 8-bit random number r is used as an address, and the corresponding 8-bit output of the ROM is assumed to be x. [0043]

Figure 11 is a block diagram showing the configuration example of the certifying means 123 in the card reader/writer shown in Figure 1. In Figure 11, the cipher function 1102 ciphers a card ID (hereinafter referred to as i) input from the input terminal 1105 based on the enciphering key K provided from the input terminal 1106, and provides the obtained 256-byte enciphered text (as described later, when a card is an authorized card, the enciphered text is written to the ROM of the card I by the card reader/writer) for the selector 1103. The random number generator 1101 generates an 8-bit random number r, transmits the random number r to the card through the output terminal 1107 and also to the selector 1103. Depending on the random number r, the selector 1103 selects 1 byte from among the 256 bytes output by the cipher function 1102, and provides the selected byte for the comparator 1104. The x transmitted from the card is provided for the other input terminal of the comparator 1104 through the input terminal 1108. Then, the comparator 1104 compares the output of the selector 1103 with x, and outputs the comparison result from the output terminal 1109. When the comparator 1104 detects a matching result, the corresponding card is determined to be an authorized card. As described above, when the certifying means 123 is realized in the card reader/writer, it is not necessary to store the contents (contents of function Si) of the ROM of all cards in the card reader/writer.

[0044]

Figure 12 is a block diagram showing the embodiment of the card signature device for writing the function Si (1002 shown in Figure 10) in the ROM of the card. In Figure 12, when a card to which a card ID is written in advance is inserted into the card interface (hereinafter referred to as an IF) 1202, the card ID is read through the card IF 1202, and the read card ID is provided for the cipher function 1201. The cipher function 1201 is a ciphering device equivalent to the cipher function 1102, ciphers the card ID based on the enciphering key K (equivalent to the enciphering key K added to the input terminal 1106 shown in Figure 11) provided from the input terminal 1203, and writes the obtained 256-byte enciphered text to the ROM forming the function Si of the card through the card IF 1202 (1102 shown in Figure 10).

[0045]

In the above-mentioned embodiment, the once writable ROM is used as ROM configuring the function Si (1002 shown in Figure 10) of the card, but any memory can be used as long as the written contents can be stored. Additionally, in the above-mentioned embodiment, the method of configuring a cipher function is not described above, but the method of configuring a cipher function is not directly related to the present invention. Therefore, any cipher function can be used. A private key ciphering can be used, or if necessary, a public key ciphering can be used. A feedback shift register can also be used. When a cipher function is configured by a feedback shift register, for example, the initial status of the feedback shift register is defined as a card ID using the coefficient of the feedback shift register as a ciphering key, and the enciphered text is defined as

the output of the feedback shift register. Furthermore, in the above-mentioned embodiment, the enciphering key K provided for the cipher function is fixed, but the enciphering key K can be periodically changed.

[0046]

In the above-mentioned embodiment, the card information about all used cards is transmitted to the center equipment, but when there is a small possibility of a forged card, only the card information about a selected part of cards can be transmitted to reduce the information to be transmitted to the center equipment. For example, only when a predetermined value is used for a hash value of a card ID, card information is transmitted. In this case, all the cards are not checked, but only a part of cards are extracted for check. When one forger produces forged cards using a number of IDs, this method effectively works to detect the forged cards.

[0047]

[Effect of the Invention]

The first effect is to reduce the communications cost because, in the conventional unauthorized use preventing system using a center, the IDs of all cards and the use histories are transmitted in realtime from a terminal to a center, and the determination results are to be received from the center as to whether or not the card is authorized. However, according to the present invention, the copy of the master black list of the center equipment is held by the card reader/writer, and when a forged card is detected using a black list, it is not necessary to communicate data with the center equipment in realtime. Furthermore, as necessary, the amount of data to be transmitted can

be reduced by transmitting the IDs and the use histories of a part of cards.

[0048]

The second effect is to reduce the device cost because, according to the present invention, card certification is employed to interpolate the detection of a forged card using a black list. Since the certifying means is simple, it is not necessary to use a complicated ciphering system in communications between a card and a card reader/writer and certification. Since the present invention requires certification of a card, it is not applicable to a magnetic card. That is, according to the present invention, only a card system using an IC card can be applicable. However, unlike the other card systems, the present invention can have the effect of preventing unauthorized use using a common inexpensive IC card loaded only with 8-bit microprocessor without using a dedicated expensive IC card loaded with a certification ciphering circuit. Therefore, now that the cost of an IC card has been reduced, the problem of the cost can be substantially ignored. Especially, in a system of paying a fare using a non-touch type IC card, the problem of the cost can be mostly ignored because of the microprocessor and the circuit for communications loaded into the cards.

[0049]

The third effect is to possibly perform a high-speed process because, as described above, it is not necessary to use a complicated ciphering system requiring a long processing time, or to communicate with the center equipment in realtime.

[0050]

The fourth effect is to have high probability of detecting a forged card because there are some possible methods of nullifying the unauthorized card use preventing technology of the present invention and using a forged card as described below, but any of the methods can not be easily realized. The first attack method is to prepare replicas of a plurality of cards by a forger to appropriately use depending on time. If all users of forged cards use specified forged cards at a specified time, and once-used cards are never used again, then a card manager cannot prevent the use of the forged cards even when the unauthorized cards are detected and the IDs of the cards are added to the black lists. However, since the forgers of the forged cards have to prepare a large number of authorized cards, it is difficult to make profits in the above-mentioned manner. Even if the forgers can sell a large number of forged cards, there is a strong possibility that the sales of the forged cards is revealed, and careless user and the mistake in using the forged cards prevent the forged cards from being used as scheduled at a predetermined time, thereby disabling a large number of forged cards to be successfully used. Therefore, if a black list is updated at appropriate time intervals, the attack method is not effective at all. The second attack method is to use a large number of forged cards to overflow a master black list or black lists and prevent the operation of the forged card use preventing method. However, at present, a storage device of a large capacity can be obtained at a low cost, and since the master black list and black lists are the lists containing IDs only, an enormous number of IDs over the number of the forged cards can be easily stored. Therefore, so far as the storage devices of

the card reader/writer and the center equipment are appropriately selected, the attack cannot successfully work.

[Brief Description of the Drawings]

Figure 1 is a block diagram showing the basic configuration of the embodiment of the card reader/writer;

Figure 2 is a flowchart for explanation of the operation relating to the detection of a forged card in the operations of the card reader/writer;

Figure 3 is a flowchart for explanation of the operation relating to the communications with the center in the operations of the card reader/writer;

Figure 4 is a block diagram showing the basic configuration of an embodiment of a card;

Figure 5 is a flowchart for explanation of the operation of a card;

Figure 6 is a block diagram showing the basic configuration of an embodiment of the center equipment;

Figure 7 is a flowchart for explanation of the operation relating to the detection of a forged card in the operations of the center equipment;

Figure 8 is a flowchart for explanation of the operation relating to the communications with the card reader/writer in the operations of the center equipment;

Figure 9 is a sequence chart for explanation of the certifying method using the certifying means of the card reader/writer and using the certifying means of a card;

Figure 10 is a block diagram showing an example of the configuration of the certifying means of a card;

Figure 11 is a block diagram showing an example of the configuration of the certifying means in the card reader/writer;

Figure 12 is a block diagram showing an embodiment of the card signature device; and

Figure 13 shows the entire configuration shoring an example of the forged card use preventing system according to the present invention.

[Description of Symbols]

1 ... card reader/writer

2 ... card

3 ... center equipment

4 ... external device

110 ... control signal interface

120, 420, 620 ... data processing device

130, 430, 630 ... storage device

140, 1202 ... card interface

150, 650 ... communicating device

410 ... interface

1002 ... function Si

1101 ... random number generator

1102, 1201 ... cipher function

1103 ... selector

1104 ... comparator

Reference 1

特開平10－187826

Figure 1
【図1】

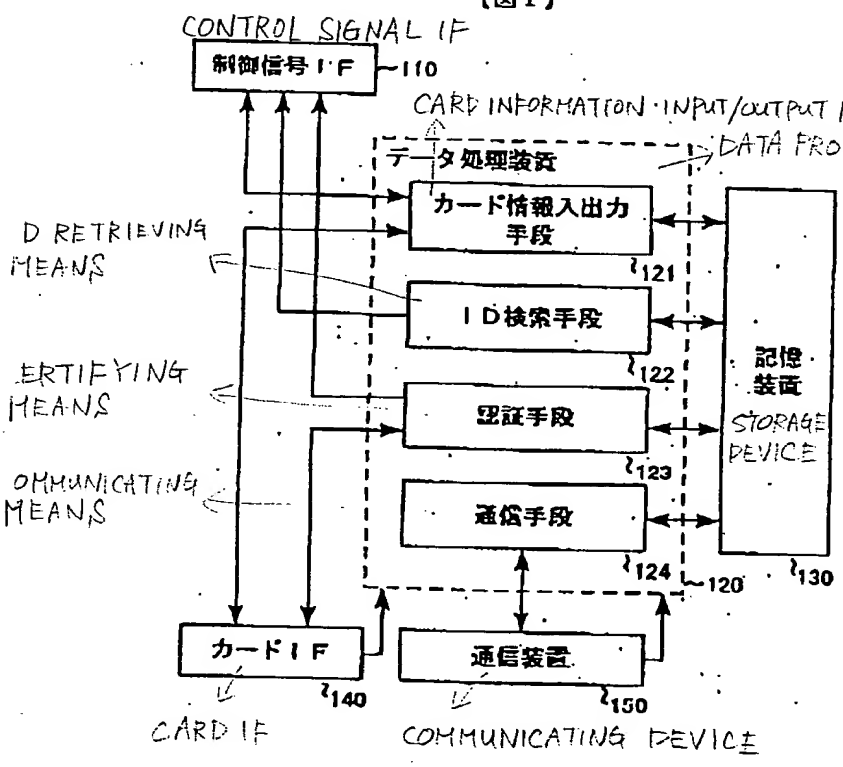


Figure 2
【図2】

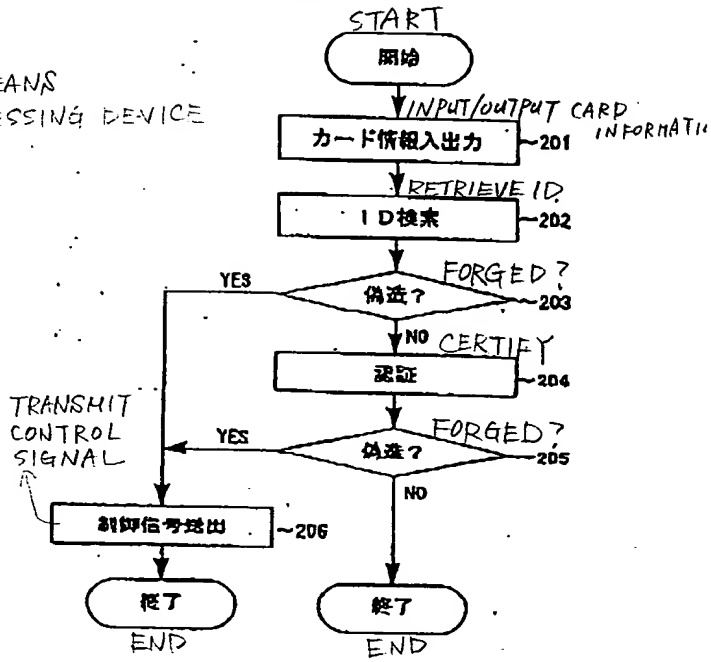


Figure 3
【図3】

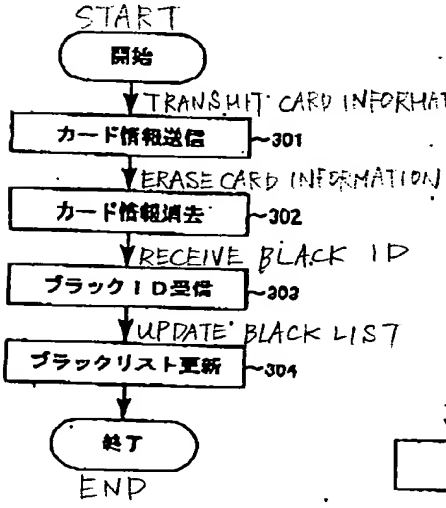


Figure4
【図4】

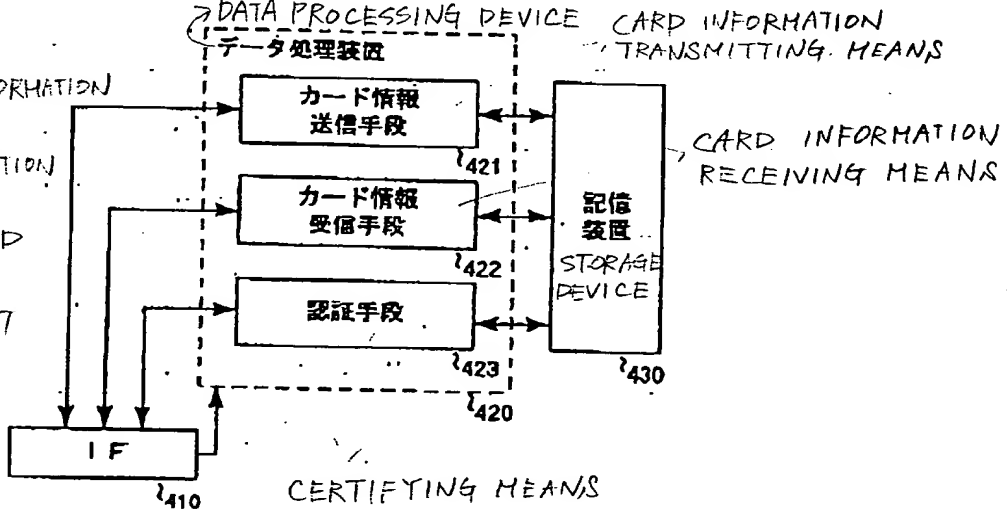


Figure 5
【図5】

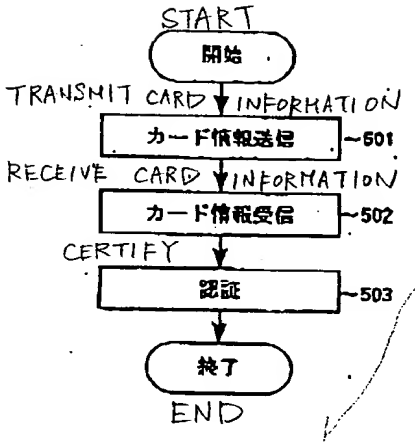


Figure 6
【図6】

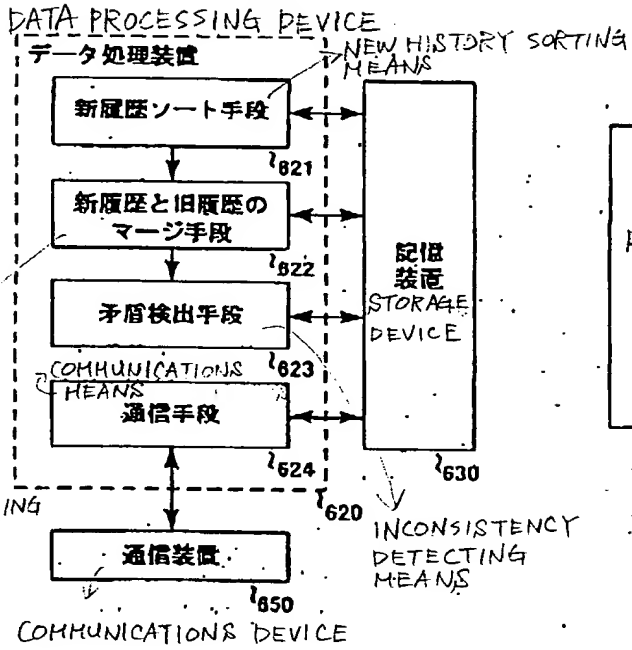


Figure 8
【図8】

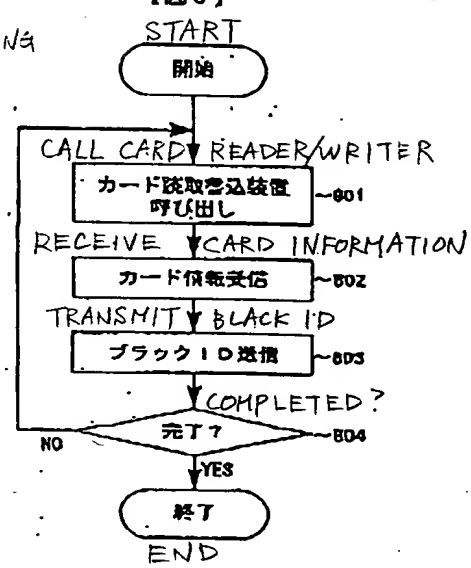


Figure 7
【図7】

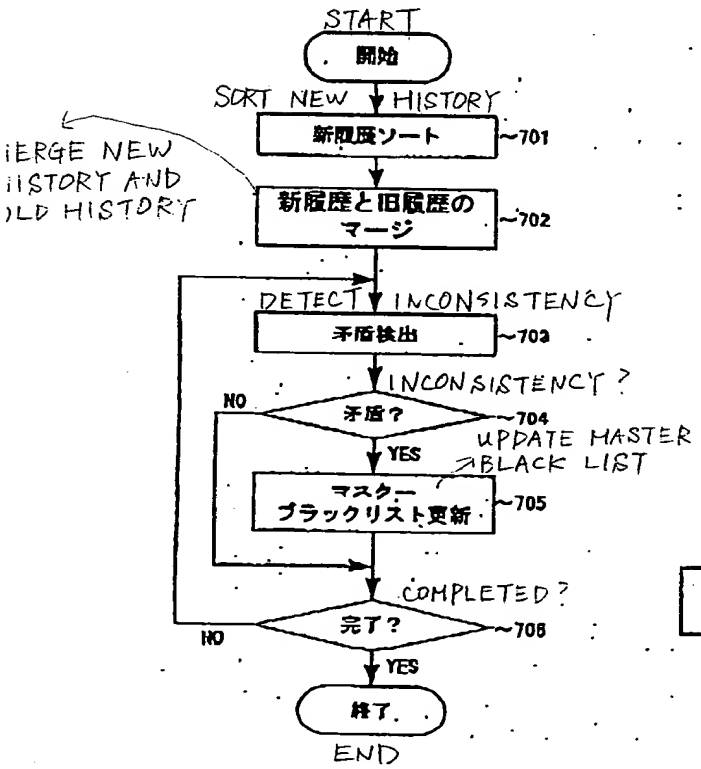


Figure 9
【図9】

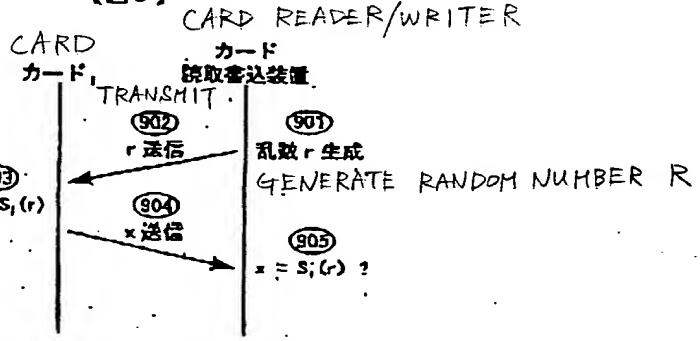


Figure 10
【図10】

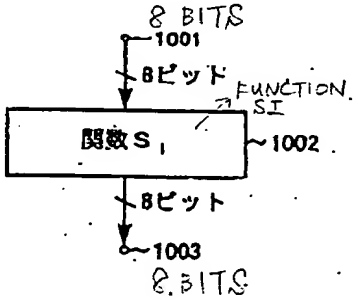


Figure 12
【図12】

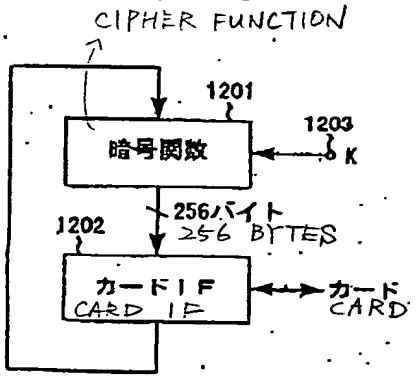


Figure 11
【図11】

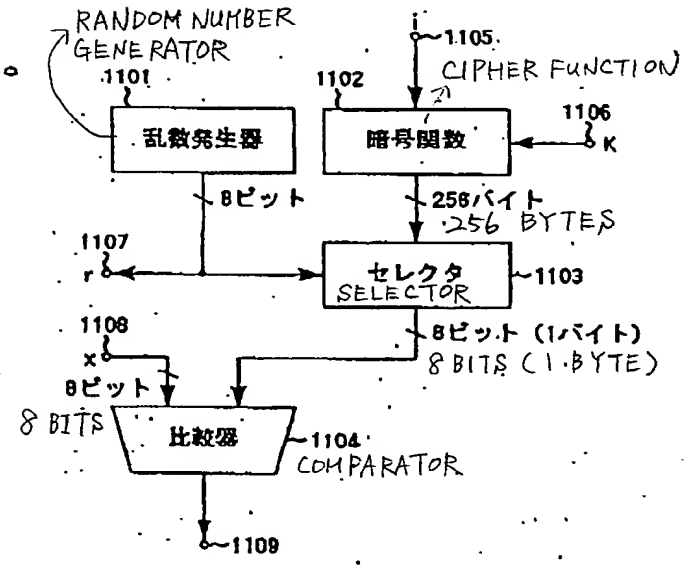
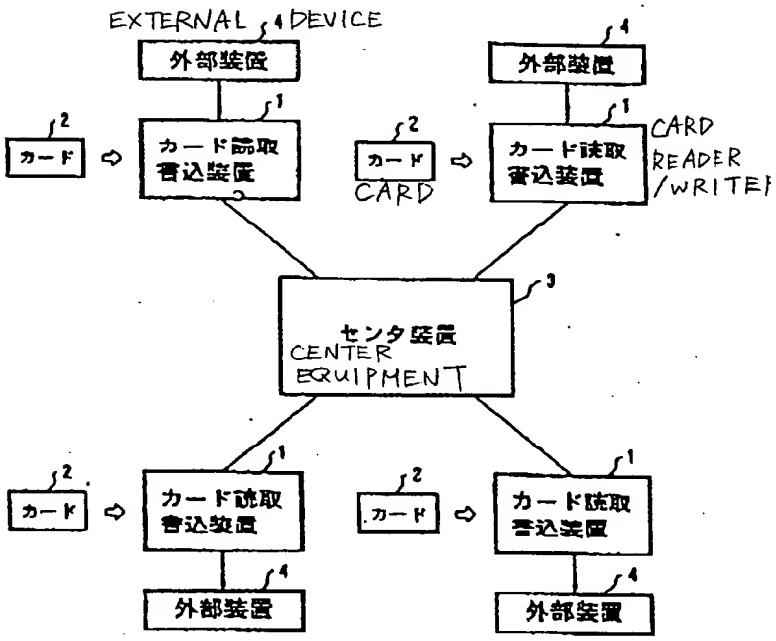


Figure 13
【図13】



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-187826
(43)Date of publication of application : 21.07.1998

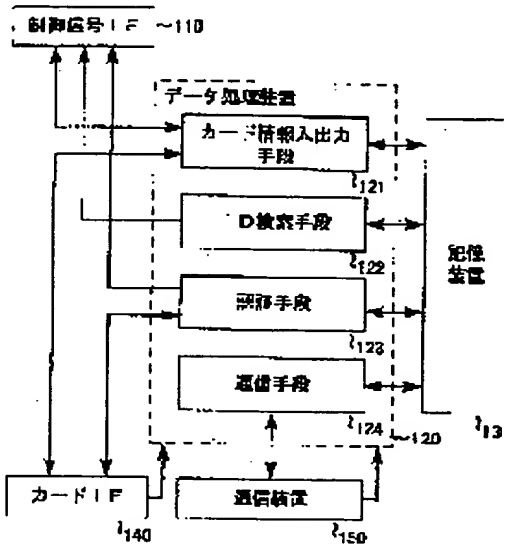
(51)Int.Cl. G06F 17/60
G06F 19/00
G06K 17/00
G07D 9/00
G07F 7/12

(21)Application number : 08-354467
(22)Date of filing : 19.12.1996

(71)Applicant : NEC CORP
(72)Inventor : SHIMADA MICHIO

(54) FORGED CARD USE PREVENTING METHOD, CARD READER/WRITER AND FORGED CARD USE PREVENTING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To make difficult the use of forged card without performing any real-time communication with center equipment and any high-level enciphering inside the card.
SOLUTION: When an IC card is used, an ID retrieving means 122 of card reader/writer investigates whether the ID of card is registered on a black list stored in a storage device 130 or not and when that ID is registered, it is discriminated as a forged card. Besides, a certifying means 123 communicates with the card to certify the card and when the card is not certified, it is discriminated as a forged card. A communicating means 124 performs non-real-time communication with center equipment, transmits card information to center equipment and receives the ID to be added to the black list from the center equipment.



LEGAL STATUS

[Date of request for examination] 19.12.1996
[Date of sending the examiner's decision of rejection] 14.11.2000
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

ASA-823

Reference 1

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－187826

(43)公開日　平成10年(1998)７月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	３４０Ｃ
19/00		Ｇ０６Ｋ　17/00	Ｓ
Ｇ０６Ｋ　17/00		Ｇ０７Ｄ　9/00	４６１Ｚ
Ｇ０７Ｄ　9/00	４６１	Ｇ０６Ｆ　15/30	３３０
Ｇ０７Ｆ　7/12		Ｇ０７Ｆ　7/08	Ｃ

審査請求　有　　請求項の数５　ＦＤ　（全 13 頁）

(21)出願番号　特願平8－354467

(22)出願日　平成８年(1996)12月19日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　島田　道雄
東京都港区芝五丁目７番１号　日本電気株式会社内

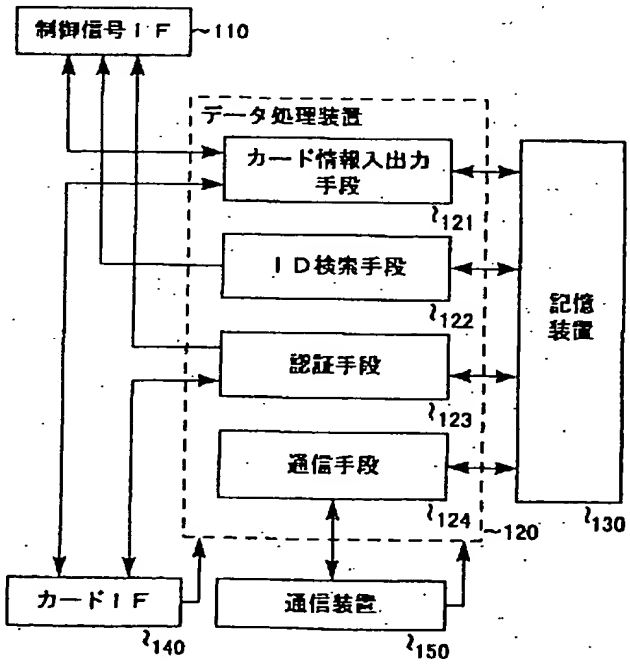
(74)代理人　弁理士　境　廣巳

(54)【発明の名称】　偽造カード使用防止方法およびカード読取書込装置ならびに偽造カード使用防止システム

(57)【要約】

【課題】　センタ装置とリアルタイムで通信しないで、また、カード内部で高度な暗号化を行わないで、偽造カードの使用を困難にする。

【解決手段】　ＩＣカードの使用時、カード読取書込装置のＩＤ検索手段１２２は、カードのＩＤが記憶装置１３０に記憶されているブラックリストに登録されているか否かを調べ、登録されていれば偽造カードであると判定する。また、認証手段１２３は、カードと通信を行ってカードを認証し、もし、カードが認証されなかったら、偽造カードであると判定する。通信手段１２４は、センタ装置と非リアルタイムで通信し、センタ装置にカード情報を送信するとともに、センタ装置からブラックリストに追加するＩＤを受信する。



1

【特許請求の範囲】

【請求項１】　カードの不正な使用を防止する方法において、

カード読取書込装置によってカードから取得したＩＤや使用履歴などのカード情報を非リアルタイムにセンタ装置に送信し、センタ装置においてカードの使用履歴の推移を評価して論理的な矛盾を含むカードのＩＤをブラックＩＤとして検出してカード読取書込装置に送信することで、カード読取書込装置の保持するブラックリストを逐次更新し、

カードの使用時は、カード読取書込装置において、そのカードのＩＤとブラックリスト中のＩＤとの比較によって不正なカードを検出すると共に、更に、カードとの通信によってそのカードが正規のものか否かを識別する認証を行うことを特徴とする偽造カード使用防止方法。

【請求項２】　カードの不正な使用を防止する機能を有するカード読取書込装置であって、

カードの使用者に対してサービスを提供する外部装置との通信を行うための制御信号インタフェースと、

カードとの通信を行うためのカードインタフェースと、

センタ装置との通信を行うための通信装置と、

前記センタ装置から送られてきた偽造カードにかかるＩＤを登録してあるブラックリストを記憶する記憶装置と、

前記カードインタフェースを介してカードに記憶されているＩＤや使用履歴などのカード情報を読み取って前記記憶装置に記憶するとともに、予め決められた手順にもとづいてカード情報を書き換えて、書き換えられたカード情報を前記カードインタフェースを介してカードに書き込むカード情報入出力手段と、

カードのＩＤが前記記憶装置に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出するＩＤ検索手段と、

前記カードインタフェースを介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出する認証手段と、

前記通信装置を介してセンタと非リアルタイムで通信して、センタに前記記憶装置に記憶されたカード情報を送信するとともに、センタから前記ブラックリストに追加するＩＤを受信する通信手段とを備えることを特徴とするカード読取書込装置。

【請求項３】　カードの不正な使用を防止するシステムにおいて、

センタ装置と、カードの使用者に対してサービスを提供する外部装置および前記センタ装置に通信可能に接続された複数のカード読取書込装置とを含み、

2

前記カード読取書込装置は、

前記外部装置との通信を行うための制御信号インタフェースと、

カードとの通信を行うためのカードインタフェースと、

記憶装置と、

前記センタ装置との通信を行うための通信装置と、

前記カードインタフェースを介してカードに記憶されているＩＤや使用履歴などのカード情報を読み取って前記記憶装置に記憶するとともに、予め決められた手順にもとづいてカード情報を書き換えて、書き換えられたカード情報を前記カードインタフェースを介してカードに書き込むカード情報入出力手段と、

カードのＩＤが前記記憶装置に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出するＩＤ検索手段と、

前記カードインタフェースを介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出する認証手段と、

前記通信装置を介してセンタと非リアルタイムで通信して、センタに前記記憶装置に記憶されたカード情報を送信するとともに、センタから前記ブラックリストに追加するＩＤを受信する通信手段とを備え、

前記センタ装置は、

前記カード読取書込装置との通信を行うための通信装置と、

記憶装置と、

該記憶装置に記憶されている新しく使われたカードの使用履歴をＩＤ順に並べ替える新履歴ソート手段と、

前記記憶装置に記憶されている過去に使われたカードの使用履歴に、前記新履歴ソート手段でソートされた、新しく使われたカードの使用履歴を追加する新履歴と旧履歴のマージ手段と、

使用履歴が追加されたカードについてカードの使用履歴の推移を評価して、論理的な矛盾が無いか否かを検出し、もし矛盾が検出されたら、そのカードのＩＤを、前記記憶装置に記憶されているマスターブラックリストに登録する矛盾検出手段と、

前記通信装置を介して前記カード読取書込装置と非リアルタイムに通信して、前記カード読取書込装置からカード情報を受信して前記記憶装置に記憶するとともに、前記マスターブラックリストに新たに登録されたＩＤを前記カード読取書込装置に送信する通信手段とを備え、

前記カードは、

前記カード読取書込装置との間の通信を行うためのインタフェースと、

記憶装置と、

該記憶装置に記憶されているＩＤや使用履歴などのカード情報を前記インタフェースを介して前記カード読取書込装置に送信するカード情報送信手段と、
新しいカード情報を前記インタフェースを介して前記カード読取書込装置から受信して前記記憶装置に書き込むカード情報受信手段と、
前記インタフェースを介して前記カード読取書込装置と通信を行ってカードの認証を行う認証手段とを備えることを特徴とする偽造カード使用防止システム。
【請求項４】　前記カード読取書込装置の認証手段は、入力される暗号鍵Ｋにもとづいて、入力されるカードＩＤを暗号化して、暗号文を出力する暗号化手段と、
乱数ｒを生成する乱数生成手段と、
該生成された乱数ｒをカードに送信して、それに対するカードの出力ｘを受信する手段と、
前記暗号化手段から出力された暗号文のうち前記生成された乱数ｒで指定される位置のビット列を選択して出力するセレクタと、
該セレクタの出力とカードの前記出力ｘを比較する比較器とを備え、
前記カードの認証手段は、
予めデータの書き込まれたメモリを備え、前記カード読取書込装置の送信した乱数ｒを前記メモリのアドレスとして、それに対応する前記メモリのデータ出力ｘを前記カード読取書込装置に送信する構成を有することを特徴とする請求項３記載の偽造カード使用防止システム。
【請求項５】　カードとの通信を行うためのカードインタフェースと、該カードインタフェースを介して署名対象カードから読み込んだカードＩＤと別途入力された暗号鍵にもとづいて前記カードＩＤを暗号化する手段とを備え、暗号化によって得られた暗号文を前記カードインタフェースを介して署名対象カードの前記メモリに書き込む構成を有するカード署名装置を備えたことを特徴とする請求項４記載の偽造カード使用防止システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、料金の支払いや身分証明のために用いられるＩＣカードを偽造して不正に使用することを防止する技術に関する。
【０００２】
【従来の技術】我々の身の回りでは、良く知られているように、磁気カードやＩＣカードが、現金や身分証明書の代替として広く使用されている。これらのカードは、しばしば、店員などの人手を介さずに、公衆電話や自動改札機や現金支払機などに投入されて使われる。そのような使われ方がされる用途では、カードの精巧な複製を製造しなくても、カードのデータを別のカードに電子的に複製することで、偽造カードが簡単に製造できるため、偽造カードを製造して不正に利益を得ようとする不心得な者が後を断たない。

【０００３】そこで、クレジットカードでは、センタにカードのＩＤや有効期限や所有者名や使用履歴などのカード情報を登録・照会することが行われていた。なお、ＩＤとは、それぞれのカードに予め割り当てられたカード固有の番号のことである。このようにすれば、偽造カードのＩＤが一旦センタに登録されれば、その偽造カードが使えなくなる。このようなカードの不正な使用を防止する方法としては、例えば特開平３－２５５６８号公報に記載のものがある。
【０００４】また、クレジットカードでは、カード会社しか知らない暗号鍵でＩＤなどのカード情報を暗号化して得られるデータをカードに記録することが行われていた。このようにすれば、カード会社以外の者が新しいＩＤを持つカードを不正に発行することができなくなる。このような防止方法としては、例えば特開平１－２６２８８６号公報や特開昭６２－１８８７０号公報に記載のものがある。
【０００５】なお、カードの偽造には、正規のカードと同じものを複製するものや、正規のカードのデータを書き換えてカードの価値を大きくするものや（狭義には変造と呼ぶ）、新しいＩＤを持つカードを製造するものがあるが（狭義には偽造と呼ぶ）、以下では特に断りの無い限り、すべてを偽造と呼ぶことにする。
【０００６】また、認証とは、カードと通信することによって、そのカードが正規のものか否かを識別する技術である。暗号とは、暗号鍵に依存して、データ（平文と呼ぶ）を別のデータ（暗号文と呼ぶ）に変換するもので、暗号文から平文が容易に推定できず、また、平文と暗号文から暗号鍵が容易に推定できないような変換のことである。なお、認証や暗号については、例えば、昭晃堂から１９９０年に発行された辻井，笠原編著「暗号と情報セキュリティ」などに詳しい解説がある。
【０００７】
【発明が解決しようとする課題】センタを設置して、カードの使用履歴を問い合わせることで、偽造カードの使用を検出する方法は、クレジットカードならともかく、小額の支払いに用いられるカードシステムには、通信コスト上の問題があるので適用できないという問題があったし、交通料金の支払いに用いられるカードシステムのように短時間で処理しなければならないカードシステムには、センタとの通信に時間がかかるために、適用できないという問題があった。
【０００８】また、カードのＩＤを暗号化して記録する従来の方法では、偽造者がＩＤを自由に選択することは防げるものの、カードを複製して偽造カードを製造することは防げないため、そのような不正な使用を防止することはできなかった。
【０００９】また、認証によってのみカードの不正な使用を防止する方法は、防止効果を高めるために、暗号化のための複雑な処理や多桁整数の四則演算を必要とする

ので、ＩＤカードに搭載されている８ビットのマイクロコンピュータで高速処理することは困難であるという問題があった。

【００１０】本発明は、以上の問題点を解決し、運用コストが小さくて高速に処理できる偽造カード使用防止技術を提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明は、偽造カードの使用を防止する方法において、カード読取書込装置（図１３の１）によってカード（図１３の２）から取得したＩＤや使用履歴などのカード情報を非リアルタイムにセンタ装置（図１３の３）に送信し、センタ装置においてカードの使用履歴の推移を評価して論理的な矛盾を含むカードのＩＤをブラックＩＤとして検出してカード読取書込装置に送信することで、カード読取書込装置の保持するブラックリストを逐次更新し、カードの使用時は、カード読取書込装置において、そのカードのＩＤとブラックリスト中のＩＤとの比較によって不正なカードを検出すると共に、更に、カードとの通信によってそのカードが正規のものか否かを識別する認証を行うことを特徴とする。

【００１２】また、カードの不正な使用を防止する機能を有する本発明のカード読取書込装置は、カードの使用者に対してサービスを提供する外部装置（図１３の４）との通信を行うための制御信号インタフェース（図１の１１０）と、カードとの通信を行うためのカードインタフェース（図１の１４０）と、センタ装置との通信を行うための通信装置（図１の１５０）と、前記センタ装置から送られてきた偽造カードにかかるＩＤを登録してあるブラックリストを記憶する記憶装置（図１の１３０）と、前記カードインタフェースを介してカードに記憶されているＩＤや使用履歴などのカード情報を読み取って前記記憶装置に記憶するとともに、予め決められた手順にもとづいてカード情報を書き換えて、書き換えられたカード情報を前記カードインタフェースを介してカードに書き込むカード情報入出力手段（図１の１２１）と、カードのＩＤが前記記憶装置に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出するＩＤ検索手段（図１の１２２）と、前記カードインタフェースを介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出する認証手段（図１の１２３）と、前記通信装置を介してセンタと非リアルタイムで通信して、センタに前記記憶装置に記憶されたカード情報を送信するとともに、センタから前記ブラックリストに追加するＩＤを受信する通信手段（図１の１２４）とを備えることを特徴とする。

【００１３】また、本発明は、偽造カードの使用を防止するシステムにおいて、センタ装置（図１３の３）と、カード（図１３の２）の使用者に対してサービスを提供する外部装置（図１３の４）および前記センタ装置に通信可能に接続された複数のカード読取書込装置（図１３の１）とを含み、前記カード読取書込装置は、前記外部装置との通信を行うための制御信号インタフェース（図１の１１０）と、カードとの通信を行うためのカードインタフェース（図１の１４０）と、記憶装置（図１の１３０）と、前記センタ装置との通信を行うための通信装置（図１の１５０）と、前記カードインタフェースを介してカードに記憶されているＩＤや使用履歴などのカード情報を読み取って前記記憶装置に記憶するとともに、予め決められた手順にもとづいてカード情報を書き換えて、書き換えられたカード情報を前記カードインタフェースを介してカードに書き込むカード情報入出力手段（図１の１２１）と、カードのＩＤが前記記憶装置に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出するＩＤ検索手段（図１の１２２）と、前記カードインタフェースを介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を前記制御信号インタフェースに送出する認証手段（図１の１２３）と、前記通信装置を介してセンタと非リアルタイムで通信して、センタに前記記憶装置に記憶されたカード情報を送信するとともに、センタから前記ブラックリストに追加するＩＤを受信する通信手段（図１の１２４）とを備え、前記センタ装置は、前記カード読取書込装置との通信を行うための通信装置（図６の６５０）と、記憶装置（図６の６３０）と、該記憶装置に記憶されている新しく使われたカードの使用履歴をＩＤ順に並べ替える新履歴ソート手段（図６の６２１）と、前記記憶装置に記憶されている過去に使われたカードの使用履歴に、前記新履歴ソート手段でソートされた、新しく使われたカードの使用履歴を追加する新履歴と旧履歴のマージ手段（図６の６２２）と、使用履歴が追加されたカードについてカードの使用履歴の推移を評価して、論理的な矛盾が無いか否かを検出し、もし矛盾が検出されたら、そのカードのＩＤを、前記記憶装置に記憶されているマスターブラックリストに登録する矛盾検出手段（図６の６２３）と、前記通信装置を介して前記カード読取書込装置と非リアルタイムに通信して、前記カード読取書込装置からカード情報を受信して前記記憶装置に記憶するとともに、前記マスターブラックリストに新たに登録されたＩＤを前記カード読取書込装置に送信する通信手段（図６の６２４）とを備え、前記カードは、前記カード読取書込装置との間の通信を行うためのインタフェース（図４の４１０）と、記憶装置（図４の４３０）と、該

記憶装置に記憶されているＩＤや使用履歴などのカード情報を前記インタフェースを介して前記カード読取書込装置に送信するカード情報送信手段（図４の４２１）と、新しいカード情報を前記インタフェースを介して前記カード読取書込装置から受信して前記記憶装置に書き込むカード情報受信手段（図４の４２２）と、前記インタフェースを介して前記カード読取書込装置と通信を行ってカードの認証を行う認証手段（図４の４２３）とを備えることを特徴とする。

【００１４】また、前記カード読取書込装置の認証手段は、入力される暗号鍵Ｋにもとづいて、入力されるカードＩＤを暗号化して、暗号文を出力する暗号化手段（図１１の１１０２）と、乱数ｒを生成する乱数生成手段（図１１の１１０１）と、該生成された乱数ｒをカードに送信して、それに対するカードの出力ｘを受信する手段（図１１の１１０７，１１０８）と、前記暗号化手段から出力された暗号文のうち前記生成された乱数ｒで指定される位置のビット列を選択して出力するセレクタ（図１１の１１０３）と、該セレクタの出力とカードの前記出力ｘを比較する比較器（図１１の１１０４）とを備え、前記カードの認証手段は、予めデータの書き込まれたメモリ（図１０の１００２）を備え、前記カード読取書込装置の送信した乱数ｒを前記メモリのアドレスとして、それに対応する前記メモリのデータ出力ｘを前記カード読取書込装置に送信する構成を有することを特徴とする。

【００１５】さらに、カードとの通信を行うためのカードインタフェース（図１２の１２０２）と、該カードインタフェースを介して署名対象カードから読み込んだカードＩＤと別途入力された暗号鍵にもとづいて前記カードＩＤを暗号化する手段（図１２の１２０１）とを備え、暗号化によって得られた暗号文を前記カードインタフェースを介して署名対象カードの前記メモリに書き込む構成を有するカード署名装置を備えている。

【００１６】

【作用】従来の偽造カード使用防止技術は、偽造カードの使用が確実に検出できることを目指して設計されていた。しかしながら、偽造カードの使用を確実に検出しようとするからこそ、その不正使用を防止するためのコストが大きくなったり、不正使用の検出に要する時間が長くなると考えられる。そこで、本発明では、発想を転換して、偽造カードの使用を大きな確率で検出できればよしとする。もちろん、クレジット・カードのように、１回あたりの取引額が大きいシステムの場合には、偽造カードの使用者が高額な商品を大量に購入して行方をくらます可能性もあるので、偽造カードの使用を確実に検出しなければならないが、１回あたりの取引額が小さいシステム（市内バスや地下鉄などのプリペイドカードシステム等）の場合には、偽造カードの使用を確実に検出する必要はないのである。なぜなら、１回あたりの取引額が小さい場合には、偽造カードの使用者は、一般に、不正に得られる利益を大きくするために頻繁に偽造カードを使用するので、１回の使用につき或る程度の確率で偽造カードの使用が検出できれば、いつかは偽造カードの使用が検出できるからである。しかも、偽造カードの使用者を拘束できるシステム（例えばカードで交通機関の運賃を支払うようなシステム）においては、偽造カードの使用者から罰金を徴収することによって、偽造カードの使用による過去の損失も補填できるからである。もちろん、偽造カードの使用を確実に検出できないと、少数の使用者が偽造カードを稀に使用している場合には、偽造カードの使用を高い確率で見逃してしまうかもしれない。例えば、悪意を持つ正規の使用者が、プリペイドカードの残高がほとんどゼロになった時に、カードに記録されている残高の額を大きくすれば、そのカードは１回あるいは何回か不正使用されてしまうかもしれない。しかしながら、そのような場合には、偽造カードの使用による損失が極めて小さいので、たとえ検出できなくてもカード・システムの運営者の利益はほとんど損なわれない。なお、偽造カードの使用という不正行為を確率的に見逃してしまうことは、心理的には許容しがたいことかもしれないが、カード・システムの運営者の利益を考慮すると、「不正使用防止のためのコスト」を度外視して「偽造カードの使用による損失」だけを小さくするのではなく、「不正使用防止のためのコスト」と「偽造カードの使用による損失」との合計を小さくすべきなのである。従って、本発明によって「不正使用防止のためのコスト」が大幅に削減できるのであれば、経済的には、そのような見逃しは許容されるであろう。

【００１７】そこで、本発明では、まず、センタを用いる不正使用防止システムにおいて、偽造カードの判定基準を緩くする。すなわち、本発明におけるカード読取書込装置は、カードが入力されるごとにセンタ装置と通信するのではなく、入力されたカードのＩＤがカード読取書込装置の記憶装置に記憶されているブラックリストに登録されているか否かを調べ、もし、ブラックリストにＩＤが存在すれば偽造カードと判定する。また、カード読取書込装置は、カードのＩＤや使用履歴などのカード情報をセンタ装置に送信する。センタ装置への送信は、カード読取書込装置にカードが入力されるごとに行っても良いし、一定時間ごとに行っても良いし、カード情報が一定量だけ蓄積されてから行っても良いし、センタ装置がカード読取書込装置と通信する際に行っても良い。また、通信コストが大きい場合には、カード読取書込装置からセンタ装置へ、すべてのカードのＩＤや使用履歴などのカード情報を送信しないで、一部のカードのＩＤや使用履歴だけを送信しても良い。そして、センタ装置は、カード読取書込装置から送信されるカードのＩＤや使用履歴などのカード情報にもとづいて、偽造カードが使用されたかどうかを判定し、もし偽造カードが存在す

れば、その偽造カードのＩＤを、センタ装置側のマスターブラックリストに登録する。また、センタ装置は、カード読取書込装置と定期的に通信して、前回の通信から現時点までにマスターブラックリストに加わった新しいＩＤをカード読取書込装置に送ってそのブラックリストに登録する。このようにすれば、カード読取書込装置とセンタ装置とがリアルタイムで通信する必要が無くなるので、通信コストも節約できるし、不正使用の判定に要する時間も短く済む。もちろん、以上のようにすると、偽造カードのＩＤがカード読取書込装置側のブラックリストに登録されるまで、その偽造カードの使用を見逃してしまうのだが、カードを１回使用するごとに取り引きされる金額が小さく、ブラックリストの更新時間の間隔が長くなければ、偽造カードによる損害を無視できるほど小さく抑えられる。

【００１８】もっとも、以上のような「センタを用いた不正使用防止方法」は、十分な防止効果を持っていないし、偽造カードが大量に使われると経済的な損失を受けるだけでなくカードシステムを正常に運営すること自体が困難になる。というのも、本発明においては、カード読取書込装置のブラックリストは瞬時に更新されないので、カードの偽造者が、正規のカードとカード読取書込装置の間の通信を盗聴し、盗聴によって得られたカード情報にもとづいて偽造カードを作成して、その偽造カードを使うことが考えられるからである。非接触型のＩＣカードを用いたカードシステムでは、盗聴による偽造は容易である。もちろん、その偽造カードは、ブラックリストが更新されるまでしか、正規のカードとして通用しない。しかしながら、それ故に、カードの偽造者は、多くのＩＤを取得して多数の偽造カードを製造することになる。そして、それらの偽造カードが使われて、それらのＩＤがカード読取書込装置のブラックリストに登録されてしまうと、多数の正規のカードが使えなくなってしまう。カードの偽造者によって悪用されたＩＤが非常に多いと、正規のカードを偽造カードであると判定することが頻繁に発生して、カードシステムの機能が麻痺することも考えられる。以上のような「センタを用いた不正使用防止方法」がこれまで使われなかったのも、おそらく、そのような問題があったからであろう。

【００１９】そこで、本発明では、以上で述べた「センタを用いた不正使用防止方法」に加えて、「認証を用いた不正使用防止方法」を併用することで、偽造カードの使用を検出することにする。認証を併用することは、一見すると、経済性と不正使用防止効果を両立できないように思われる。なぜなら、第１に、現在の認証技術をもってすれば、認証だけでもカードの不正使用を極めて困難にできるので、不正使用防止効果の高い認証方法を用いるのであれば、わざわざセンタを設置する必要なぞないからである。第２に、装置化の容易な簡便な認証方法を採用すれば経済性は損なわれないものの、そのような認証方法には不正使用防止の効果がほとんど無いように思われるからである。しかしながら、本発明においては、カード読取書込装置のブラックリストが更新されるまでの短い期間における偽造カードの使用が、認証によって検出できれば良いのであるし、既に述べたような理由から、偽造カードの使用が大きな確率で検出できれば十分なのであるから、簡便な認証方法を利用できる。

【００２０】

【発明の実施の形態】次に、本発明の実施例について図面を参照して詳細に説明する。

【００２１】図１３は、本発明の偽造カード使用防止システムの一例を示す全体構成図である。この例の偽造カード使用防止システムは、複数のカード読取書込装置１と、これら複数のカード読取書込装置１と有線または無線によって通信可能なセンタ装置３とから構成されている。なお、２はカードを、４はカード２の使用者に対してサービスを提供する外部装置（例えば自動販売機や改札機など）をそれぞれ示す。

【００２２】本例の偽造カード使用防止システムにおいては、各カード読取書込装置１によってカード２から取得したＩＤや使用履歴などのカード情報を非リアルタイムにセンタ装置３に送信し、センタ装置３においてカードの使用履歴の推移を評価して論理的な矛盾を含むカードのＩＤをブラックＩＤとして検出して各カード読取書込装置１に送信することで、各カード読取書込装置１の保持するブラックリストを逐次更新する。なお、カード情報中の使用履歴には、カード使用日時，使用場所を定める情報（例えば各カード読取書込装置に振られた番号など），利用金額などが含まれる。そして、カード２の使用時は、各カード読取書込装置１において、そのカードのＩＤとブラックリスト中のＩＤとの比較によって不正なカードを検出すると共に、更に、カード２との通信によってそのカードが正規のものか否かを識別する認証を行う。偽造カードと判定された場合には外部装置４に制御信号が出され、当該カードを受け付けないようにする処理や警報を発する処理などが外部装置４において行われることにより、偽造カードによる不正な使用を防止する。

【００２３】以下、カード読取書込装置１，カード２およびセンタ装置３の構成例について詳述する。

【００２４】図１は、カード読取書込装置の実施例の基本構成を示す機能ブロック図である。この実施例のカード読取書込装置は、制御信号インタフェース（以下では略して制御信号ＩＦと呼ぶ）１１０と、データ処理装置１２０と、記憶装置１３０と、カードインタフェース（以下では略してカードＩＦと呼ぶ）１４０と、通信装置１５０とから構成されている。

【００２５】制御信号ＩＦ１１０は、自動販売機や改札機などカードの使用者に対してサービスを提供する外部装置とデータ処理装置１２０との間の通信を行うための

回路である。カードＩＦ１４０は、カードとデータ処理装置１２０との間の通信を行うための回路である。記憶装置１３０は、ランダム・アクセス・メモリとリード・オンリ・メモリ（以下ではＲＯＭと呼ぶ）によって構成され、データ処理装置１２０の出力するデータを記憶したり、記憶したデータをデータ処理装置１２０に供給する。通信装置１５０は、センタとデータ処理装置１２０との間の通信を行うための装置である。

【００２６】データ処理装置１２０は、マイクロプロセッサによって構成され、予めＲＯＭに書かれた命令に従って、本カード読取書込装置全体の制御を行う。すなわち、データ処理装置１２０には、カードＩＦ１４０を介してカードに記憶されているＩＤや使用履歴などの情報を読み取って記憶装置１３０に記憶するとともに、必要ならば、自動販売機や改札機などカードの使用者に対してサービスを提供する装置から制御信号ＩＦ１１０を介して供給される料金および現在日時などの情報に基づいて、カード情報の使用履歴などを書き換えて、書き換えられたデータをカードＩＦ１４０を介してカードに書き込むカード情報入出力手段１２１と、カードのＩＤが記憶装置１３０に記憶されているブラックリストに存在するか否かを検索して、もし、存在すれば、カードが偽造カードであることを示すための制御信号を制御信号ＩＦ１１０に送出するＩＤ検索手段１２２と、カードＩＦ１４０を介してカードと通信を行ってカードを認証し、もし、カードが認証されなかったら、カードが偽造カードであることを示すための制御信号を制御信号ＩＦ１１０に送出する認証手段１２３と、通信装置１５０を介してセンタと通信して、センタに対し記憶装置１３０に記憶されたカード情報を送信するとともに、センタからブラックリストに追加するＩＤを受信してブラックリストに追加する通信手段１２４とが、予めＲＯＭに書かれた命令によって、実現されている。

【００２７】図２は、図１のカード読取書込装置の動作のうち偽造カードの検出に関する動作を説明するフローチャートである。図において、カードＩＦ１４０がカードが入力されたことを示す制御信号をデータ処理装置１２０に供給したら、データ処理装置１２０は、まず、カード情報入出力手段１２１によって、カードＩＦ１４０を介してカードに記憶されているＩＤや使用履歴などの情報を読み取って記憶装置１３０に記憶するとともに、必要ならば、自動販売機や改札機などカードの使用者に対してサービスを提供する操作から制御信号ＩＦ１１０を介して供給される料金などの情報にもとづいて、カード情報を書き換えて、書き換えられたデータをカードＩＦ１４０を介してカードに書き込む（２０１）。次に、ＩＤ検索手段１２２によって、当該カードのＩＤが記憶装置１３０に記憶されているブラックリストに存在するか否かを検索して（２０２）、もし、存在すれば、制御を手順２０６に移し、さもなくば、制御を手順２０４に移す（２０３）。

【００２８】手順２０４では、データ処理装置１２０は、認証手段１２３によって、カードＩＦ１４０を介してカードと通信を行ってカードを認証する。そして、もし、カードが認証されなかったら、制御を手順２０６に移し、さもなくば、処理を終了する（２０５）。他方、手順２０６においては、データ処理装置１２０は、カードが偽造カードであることを示すための制御信号を制御信号ＩＦ１１０に送出して、処理を終了する。

【００２９】図３は、図１のカード読取書込装置の動作のうちセンタとの通信に関する動作を説明するフローチャートである。図において、通信装置１５０がセンタからの通信が入ったことを示す制御信号をデータ処理装置１２０に供給したら、データ処理装置１２０は、通信手段１２４によって、通信装置１５０を介してセンタと通信して、記憶装置１３０に記憶されていたカード情報をセンタに送信して（３０１）、記憶装置１３０に記憶されていた上記カード情報を消去する（３０２）。次に、センタからブラックリストに追加するＩＤを受信し（３０３）、この受信したＩＤを記憶装置１３０に記憶されているブラックリストに登録して（３０４）、処理を終了する。

【００３０】図４は、カードの実施例の基本構成を示す機能ブロック図である。この実施例のカードは、インタフェース（以下では略してＩＦと呼ぶ）４１０と、データ処理装置４２０と、記憶装置４３０とから構成されている。

【００３１】ＩＦ４１０は、当該カードとカード読取書込装置との間の通信を行うための回路である。記憶装置４３０は、ランダム・アクセス・メモリとＲＯＭによって構成され、データ処理装置４２０の出力するデータを記憶したり、記憶したデータをデータ処理装置４２０に供給する。

【００３２】データ処理装置４２０は、マイクロプロセッサによって構成され、予めＲＯＭに書かれた命令に従って、当該カードの制御を行う。すなわち、データ処理装置４２０には、記憶装置４３０に記憶されているＩＤや使用履歴などの情報をＩＦ４１０を介してカード読取書込装置に送信するカード情報送信手段４２１と、新しいカード情報をＩＦ４１０を介してカード読取書込装置から受信して記憶装置４３０に書き込むカード情報受信手段４２２と、ＩＦ４１０を介してカード読取書込装置と通信を行ってカードの認証を行う認証手段４２３とが、予めＲＯＭに書かれた命令によって、実現されている。なお、認証については後で詳しく述べるが、本実施例における認証手段４２３は、複雑な処理を必要としないので、データ処理装置４２０を、処理能力の低い８ビットのマイクロプロセッサで実現できる。

【００３３】図５は、図４のカードの動作を説明するフローチャートである。図において、ＩＦ４１０を介して

カード読取書込装置から通信を要求する制御信号がデータ処理装置４２０に供給されたら、データ処理措置４２０は、カード情報送信手段４２１によって、記憶装置４３０に記憶されているＩＤや使用履歴などの情報をＩＦ４１０を介してカード読取書込装置に送信し（５０１）、次に、カード情報受信手段４２２によって、新しいカード情報をＩＦ４１０を介してカード読取書込装置から受信して記憶装置４３０に書き込む（５０２）。次に、認証手段４２３によって、ＩＦ４１０を介してカード読取書込装置と通信を行ってカードの認証を行い（５０３）、処理を終了する。なお、認証方法については後で詳しく述べるが、手順５０３における認証は、カード読取書込装置における図２の手順２０４における認証と対応するもので、同じ手順ではない。

【００３４】図６は、センタ装置の実施例の基本構成を示す機能ブロック図である。この実施例のセンタ装置は、データ処理装置６２０と、記憶装置６３０と、通信装置６５０とから構成されている。

【００３５】記憶装置６３０は、ランダム・アクセス・メモリやＲＯＭによって構成され、データ処理装置６２０の出力するデータを記憶したり、記憶したデータをデータ処理装置６２０に供給する。通信装置６５０は、データ処理装置６２０とカード読取書込装置との間の通信を行うための装置である。

【００３６】データ処理装置６２０は、マイクロプロセッサによって構成され、予めＲＯＭに書かれた命令に従って、当該センタ装置の制御を行う。すなわち、データ処理装置６２０には、記憶装置６３０に記憶されている新しく使われたカードの使用履歴をＩＤ順に並べかえる新履歴ソート手段６２１と、記憶装置６３０に記憶されている過去に使われたカードの使用履歴に、新しく使われたカードの使用履歴を追加する、新履歴と旧履歴のマージ手段６２２と、使用履歴が追加されたカードについてカードの使用履歴の推移を評価して、論理的な矛盾が無いか否かを検出し、もし矛盾が検出されたら、そのカードのＩＤを、記憶装置６３０に記憶されているマスターブラックリストに登録する矛盾検出手段６２３と、通信装置６５０を介してカード読取書込装置と通信して、カード読取書込装置からカード情報を受信して記憶装置６３０に記憶するとともに、マスターブラックリストに新たに登録されたＩＤ（ブラックＩＤ）をカード読取書込装置に送信する通信手段６２４とが、予めＲＯＭに書かれた命令によって、実現されている。

【００３７】図７は、図６のセンタ装置の動作のうち偽造カードの検出に関する動作を説明するフローチャートである。図において、データ処理装置６２０は、まず、新履歴ソート手段６２１によって、記憶装置６３０に記憶されている新しく使われたカードの使用履歴をＩＤ順に並べかえる（７０１）。次に、新履歴と旧履歴のマージ手段６２２によって、記憶装置６３０に記憶されている過去に使われたカードの使用履歴に、新しく使われたカードの使用履歴を追加する（７０２）。次に、矛盾検出手段６２３によって、使用履歴が追加されたカードで手順７０３の処理がまだ行われていないカードについて、使用履歴の推移を評価して、論理的な矛盾が無いか否かを検出し（７０３）、もし矛盾が検出されたら、制御を手順７０５に移し、さもなくば制御を手順７０６に移す（７０４）。論理的な矛盾としては、例えば、同じＩＤのカードがほぼ同時刻に別々の場所（別々のカード読取書込装置）で使用されているといったことがあげられる。

【００３８】次に、手順７０５では、矛盾の検出されたカードのＩＤを、記憶装置６３０に記憶されているマスターブラックリストに登録し（７０５）、制御を手順７０６に移す。手順７０６では、使用履歴が追加されたすべてのカードについて手順７０３が実行されたか否かを調べ、もし、使用履歴が追加されたすべてのカードについて手順７０３が実行済みであれば、処理を終了し、さもなくば、制御を７０３に移す。

【００３９】図８は、図６のセンタ装置の動作のうちカード読取書込装置との間の通信に関する動作を説明するフローチャートである。図において、データ処理装置６２０は、まず、通信手段６２４によって、通信装置６５０を介して、カード読取書込装置との通信を開始し（８０１）、次に、カード読取書込装置から新しく使われたカードのカード情報を受信し（８０２）、次に、マスターブラックリストに新たに登録されたブラックＩＤをカード読取書込装置に送信し（８０３）、すべてのカード読取書込装置との交信が実行されたか否かを調べ、もし、すべてのカード読取書込装置との交信が実行済みであれば、処理を終了し、さもなくば、新しいカード読取書込装置を選択して、制御を８０１に移す（８０４）。

【００４０】次に、カード読取書込装置とカードとの間において行われる認証について説明する。

【００４１】図９は、図１のカード読取書込装置の認証手段１２３および図４のカードの認証手段４２３において用いられている認証方法を説明するシーケンスチャートである。図において、まず、カード読取書込装置が乱数ｒを生成して（９０１）、乱数ｒをカードｉに送信する（９０２）。なお、ここで、ｉはこのカードのＩＤとする。そして、カードｉは、カード読取書込装置から乱数ｒを受信し（９０２）、乱数ｒを関数S_iに入力して得られる出力ｘを求め（９０３）、ｘをカード読取書込装置に送信する（９０４）。カード読取書込装置は、ｘを受信して（９０４）、乱数ｒを関数S_iに入力して得られる出力とｘとを比較し（９０５）、もし、等しければ、通信相手のカードは正規のカードであると判定し、さもなくば、通信相手のカードは偽造カードであると判定する。なお、関数S_iはカードｉに固有な関数で、カードｉは、関数S_iだけを持っており、カード読取書込

装置は、すべてのｉについて、カードｉの関数Ｓｉを持っている。

【００４２】図１０は、図４のカードの認証手段４２３の構成例を示す機能ブロック図である。本発明においては、カードが１回使用されるごとに確実にではなく或る程度の確率で偽造カードが検出できれば良いから、関数Ｓｉの入出力ビット数を小さくできる。図の実施例では、関数Ｓｉは、カード読取書込装置から送信された８ビットの乱数ｒを入力端子１００１を介して関数Ｓｉ１００２に入力して、出力端子１００３に出力される８ビットの出力ｘをカード読取書込装置に送信している。なお、関数Ｓｉの入出力ビット数が僅か８ビットなので、関数Ｓｉ１００２は、僅か２５６バイトの（１バイトは８ビットとする）ＲＯＭ（１回書き込み可能なＲＯＭ）で構築できる。つまり、ＲＯＭ中に２５６バイトの関数Ｓｉを保持し、８ビットの乱数ｒをアドレスとして、それに対応するＲＯＭの８ビットの出力をｘとする。

【００４３】図１１は、図１のカード読取書込装置における認証手段１２３の構成例を示す機能ブロック図である。図において、暗号関数１１０２は、入力端子１１０６から供給される暗号鍵Ｋにもとづいて、入力端子１１０５から入力されるカードＩＤ（以下ではｉとする）に対して暗号化を施して、得られた長さ２５６バイトの暗号文（後述するように正規のカードの場合は、この暗号文がカード署名装置によってカードｉの上記ＲＯＭに書き込まれている）を、セレクタ１１０３に供給する。乱数発生器１１０１は、８ビットの乱数ｒを発生して、乱数ｒを出力端子１１０７を介してカードに送信するとともに、セレクタ１１０３にも供給する。セレクタ１１０３は、乱数ｒに依存して、暗号関数１１０２の出力する２５６バイトのうち１バイトを選択して、選択されたバイトを比較器１１０４に供給する。比較器１１０４のもう一方の入力には、カードから送信されたｘが入力端子１１０８を介して供給されている。そして、比較器１１０４は、セレクタ１１０３の出力とｘとを比較して、比較結果を出力端子１１０９から出力する。比較器１１０４が一致を検出した場合、当該カードは正規のカードあると判定される。以上のようにして、カード読取書込装置における認証手段１２３を実現すれば、カード読取書込装置にすべてのカードのＲＯＭの内容（関数Ｓｉの内容）を記憶する必要が無い。

【００４４】図１２は、カードのＲＯＭに関数Ｓｉ（図１０の１００２）を書き込むためのカード署名装置の実施例を示す機能ブロック図である。図において、予めカードＩＤの書き込まれているカードが、カードインタフェース（以下ではカードＩＦと呼ぶ）１２０２に差し込まれると、カードＩＦ１２０２を介して、カードＩＤが読み込まれて、読み込まれたカードＩＤが暗号関数１２０１に供給される。暗号関数１２０１は、図１１の暗号関数１１０２と等価な暗号装置で、入力端子１２０３から供給される暗号鍵Ｋ（図１１の入力端子１１０６に加わる暗号鍵Ｋと等価）にもとづいて、カードＩＤに暗号化を施して、得られた２５６バイトの暗号文を、カードＩＦ１２０２を介して、カードの関数Ｓｉ（図１０の１００２）を構成しているＲＯＭに書き込まれる。

【００４５】なお、以上の実施例においては、カードの関数Ｓｉ（図１０の１００２）を構成しているＲＯＭとして、１回書き込み可能なＲＯＭを用いたが、書き込んだ内容を保存できるものであれば、どのようなメモリを用いてもよい。また、以上の実施例においては、暗号関数の構成方法については述べなかったが、暗号関数の構成方法は、本発明と直接関係ないので、任意の暗号関数が使える。秘密鍵暗号を用いても良いし、必要ならば、公開鍵暗号を用いても良いし、フィードバック・シフトレジスタを用いても良い。なお、暗号関数をフィードバック・シフトレジスタで構成する場合には、例えば、フィードバック・シフトレジスタの係数を暗号鍵として、フィードバック・シフトレジスタの初期状態をカードＩＤとし、暗号文をフィードバック・シフトレジスタの出力とすれば良い。また、以上の実施例においては、暗号関数に供給する暗号鍵Ｋを固定として考えていたが、暗号鍵Ｋを定期的に変更しても良い。

【００４６】また、以上の実施例においては、使用されたすべてのカードのカード情報をセンタ装置に送信していたが、偽造される危険性が少ない用途においては、選択された一部のカードのカード情報だけを送信することにより、センタ装置に送信する情報を削減することも可能である。例えば、カードＩＤのハッシュ値が予め定められた値をとるものについてだけ、カード情報を送信するのである。これは、すなわち、カード全体を検査するのではなく、一部のカードだけを抜き打ち検査するということである。一人の偽造者が、多数のＩＤを利用して、偽造カードを製造している場合には、この方法でも、偽造カードを効果的に検出できる。

【００４７】

【発明の効果】第１の効果は、通信コストが小さく済むということである。なぜなら、センタを用いる従来の不正使用防止システムにおいては、端末からセンタに、すべてのカードのＩＤと使用履歴をリアルタイムで送信し、そのカードが正規のものかどうかの判定結果をセンタから受信しなければならなかったが、本発明においては、センタ装置のマスターブラックリストの移しを各カード読取書込装置が保持しており、ブラックリストによる偽造カードの検出に際して、センタ装置とリアルタイムで送信する必要がないからである。また、必要に応じて、一部のカードのＩＤと使用履歴だけを送信することで、送信するデータの量を削減できるからである。

【００４８】第２の効果は、装置コストが小さくて済むということである。なぜなら、本発明は、ブラックリストによる偽造カードの検出を補完するためにカードの認

証を導入しており、認証手段は簡便なもので済むため、カードとカード読取書込装置との通信や認証において、複雑な暗号方式を使う必要が無いからである。もっとも、本発明は、カードの認証を行わなければならないので、磁気カードには適用できない。すなわち、本発明は、ＩＣカードを用いたカードシステムにしか適用できない。しかしながら、本発明は、他のカードシステムと違い、認証暗号回路の搭載されている専用の高価なＩＣカードを使わなくとも、８ビットのマイクロプロセッサしか搭載されていない汎用の安価なＩＣカードでも、高い不正使用防止効果が発揮できるので、ＩＣカードのコストが低下している今日においては、コストの問題はほとんど無視できる。特に、非接触型のＩＣカードを使用した交通料金を支払うようなシステムにおいては、多くの場合、マイクロプロセッサや通信のための回路が搭載されているので、コストの問題はほとんど無視できる。

【００４９】第３の効果は、高速に処理できるということである。なぜなら、既に述べたように、処理時間のかかる複雑な暗号方式を使う必要もないし、センタ装置とリアルタイムで通信する必要も無いからである。

【００５０】第４の効果は、偽造カードの検出能力が高いということである。なぜなら、本発明のカード不正使用防止技術を無効にして、偽造カードを使用する方法は、以下で述べるように、原理的にはいくつか考えられるが、いずれの方法も、実際に実行することは難しいからである。第１の攻撃方法としては、偽造カードの使用者が、予め複数のカードの複製を作成しておき、それらを時間に応じて使い分けることが考えられる。もし、偽造カードの使用者のすべてが決められた時間に決められた偽造カードを使用し、一旦使用した偽造カードを２度と使わないようにすれば、カードの運営者が偽造カードの使用を検出してそのカードのＩＤをブラックリストに加えても、偽造カードの使用は防止できない。しかしながら、偽造カードの製造者は正規のカードを大量に調達しなければならないので、偽造カードの製造者が利益を得ることは難しい。また、仮に、偽造カードを大量生産して販売したとしても、カードの販売が発覚する危険が高くなるし、使用者の不注意や偽造カードを使用する時間のミスなどで、決められた時間に決められた偽造カードが使われないことが高い確率で生じ、多くの偽造カードの多くが使えなくなる。従って、ブラックリストが更新される時間の間隔が適切であれば、この攻撃方法は有効ではない。第２の攻撃方法は、大量の偽造カードを使用して、マスターブラックリストやブラックリストをオーバーフローさせて、偽造カード使用防止方法の運用を妨害する方法である。しかしながら、今日では大容量の記憶装置が安価に入手できるし、マスターブラックリストやブラックリストはＩＤだけのリストであるから、偽造カードの数を上回る膨大な数のＩＤを容易に記憶できる。従って、カード読取書込装置およびセンタ装置の記憶装置の記憶容量が適切に選択されていれば、そのような攻撃を実行するのは困難である。

【図面の簡単な説明】

【図１】カード読取書込装置の実施例の基本構成を示す機能ブロック図である。

【図２】カード読取書込装置の動作のうち偽造カードの検出に関する動作を説明するフローチャートである。

【図３】カード読取書込装置の動作のうちセンタとの通信に関する動作を説明するフローチャートである。

【図４】カードの実施例の基本構成を示す機能ブロック図である。

【図５】カードの動作を説明するフローチャートである。

【図６】センタ装置の実施例の基本構成を示す機能ブロック図である。

【図７】センタ装置の動作のうち偽造カードの検出に関する動作を説明するフローチャートである。

【図８】センタ装置の動作のうちカード読取書込装置との間の通信に関する動作を説明するフローチャートである。

【図９】カード読取書込装置の認証手段およびカードの認証手段において用いられている認証方法を説明するシーケンスチャートである。

【図１０】カードの認証手段の構成例を示す機能ブロック図である。

【図１１】カード読取書込装置における認証手段の構成例を示す機能ブロック図である。

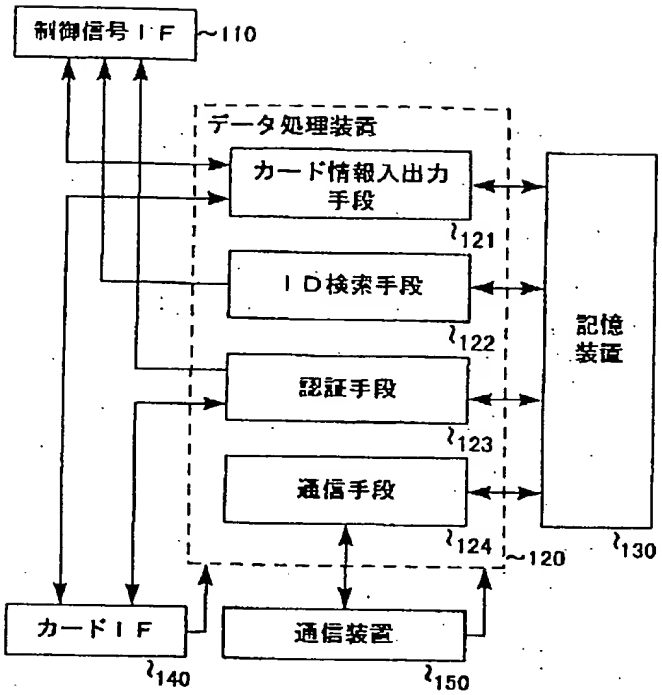
【図１２】カード署名装置の実施例を示す機能ブロック図である。

【図１３】本発明の偽造カード使用防止システムの一例を示す全体構成図である。

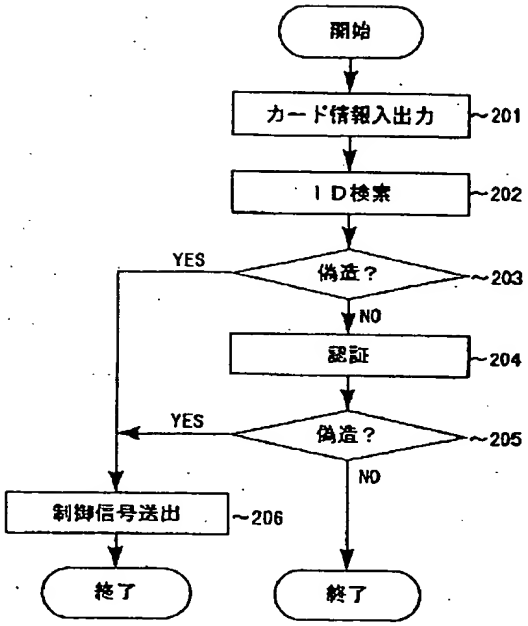
【符号の説明】

１…カード読取書込装置
２…カード
３…センタ装置
４…外部装置
１１０…制御信号インタフェース
１２０，４２０，６２０…データ処理装置
１３０，４３０，６３０…記憶装置
１４０，１２０２…カードインタフェース
１５０，６５０…通信装置
４１０…インタフェース
１００２…関数S_1
１１０１…乱数発生器
１１０２，１２０１…暗号関数
１１０３…セレクタ
１１０４…比較器

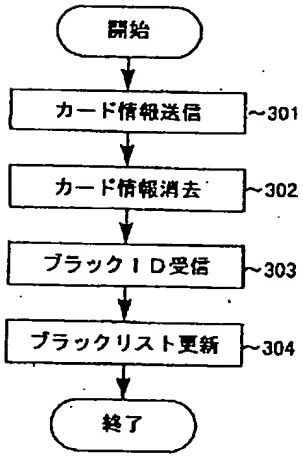
【図１】


制御信号ＩＦ
110
データ処理装置
カード情報入出力手段
121
ＩＤ検索手段
122
認証手段
123
通信手段
124
120
記憶装置
130
カードＩＦ
140
通信装置
150

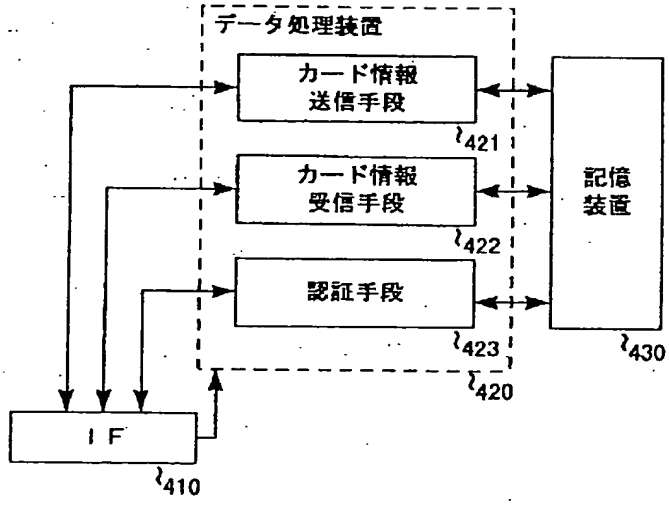
【図２】


開始
カード情報入出力
201
ＩＤ検索
202
YES
偽造？
203
NO
認証
204
YES
偽造？
205
NO
制御信号送出
206
終了
終了

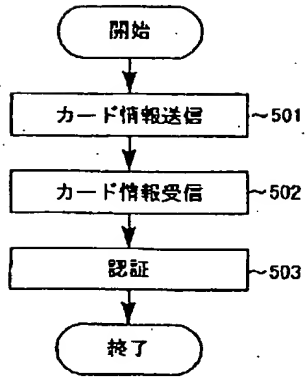
【図３】


開始
カード情報送信
301
カード情報消去
302
ブラックＩＤ受信
303
ブラックリスト更新
304
終了

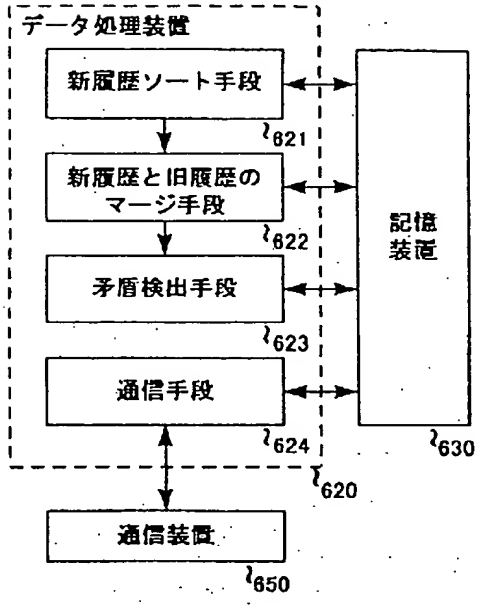
【図４】


データ処理装置
カード情報送信手段
421
カード情報受信手段
422
認証手段
423
420
記憶装置
430
ＩＦ
410

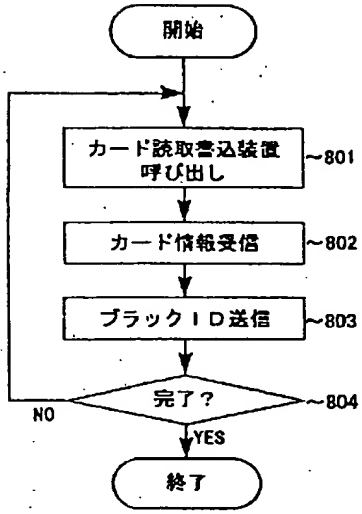
【図５】



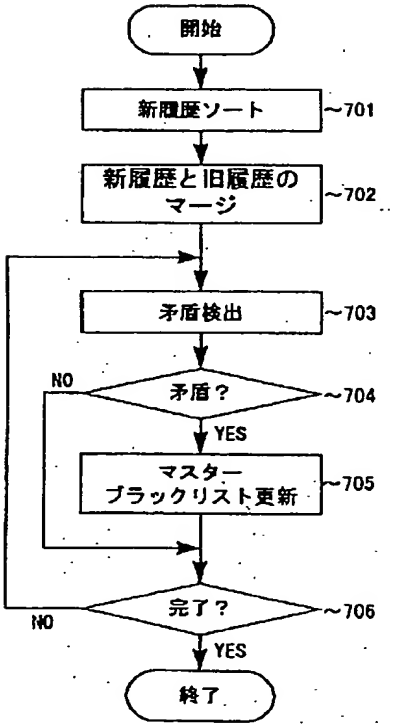
【図６】



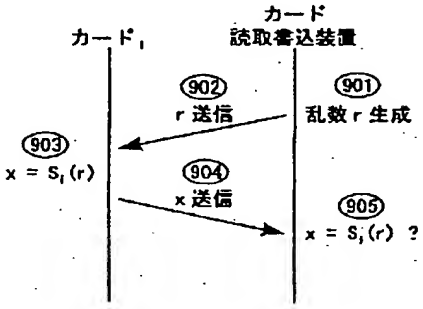
【図８】



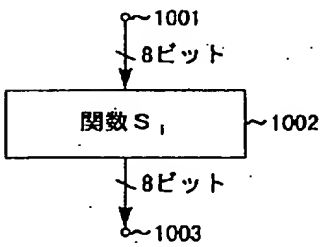
【図７】



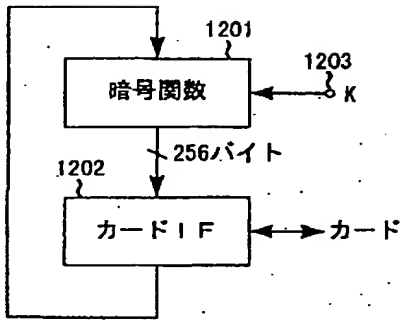
【図９】



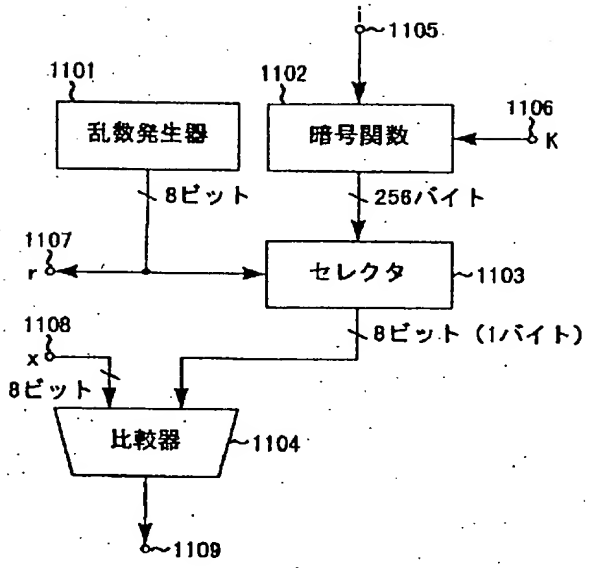
【図１０】



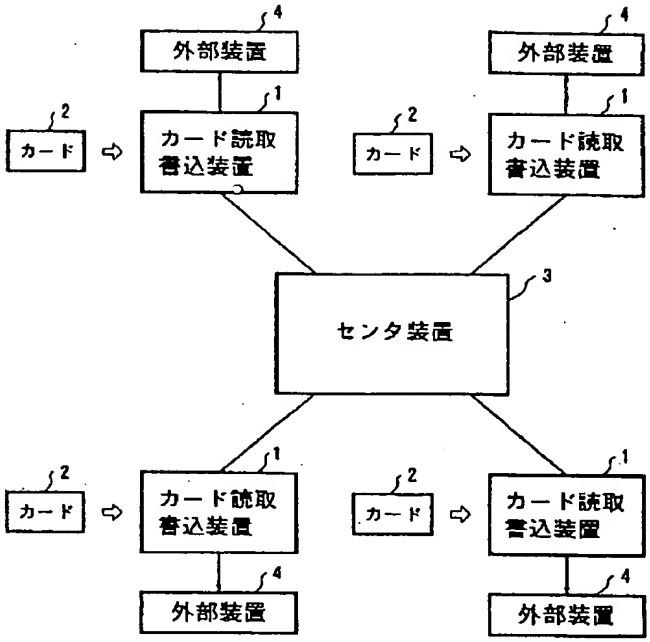
【図１２】



【図１１】


1105
1101
1102
乱数発生器
暗号関数
1106
K
8ビット
256バイト
1107
r
セレクタ
1103
8ビット（1バイト）
1108
x
8ビット
比較器
1104
1109

【図１３】


外部装置
4
カード
2
カード読取
書込装置
1
センタ装置
3